# Table of Contents

Welcome to Tenable.ad ........................................................................................................ 7  
Get Started with Tenable.ad 3.x User and Administrator Guide ........................................ 8  
Connection to Tenable.ad ................................................................................................... 10  
User Preferences .................................................................................................................. 12  
Navigate Tenable.ad 3.x User and Administrator Guide .................................................... 14  
Notifications ....................................................................................................................... 18  
Dashboards ........................................................................................................................... 21  
Widgets ................................................................................................................................... 23  
Topology ............................................................................................................................... 28  
  Understand Trust Relationships Color Code ........................................................................ 30  
  Trust Relationships .............................................................................................................. 31  
  Dangerous Trusts .................................................................................................................... 34  
Trail Flow ............................................................................................................................... 35  
  View the Real-Time Monitoring of Your AD Infrastructures .............................................. 38  
  Pause and Restart the Trail Flow .......................................................................................... 42  
  Filter the Real-Time Flow of Events ................................................................................... 44  
  Run a Search in the Trail Flow ............................................................................................ 45  
    Build Faster Queries Using the Wizard ............................................................................ 50  
    Search Manually ............................................................................................................... 59  
    Show Only Deviant Events ................................................................................................ 62  
History blade .......................................................................................................................... 64  
Bookmarks Blade ..................................................................................................................... 66  

Copyright © 2022 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
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Forests and Domains</td>
<td>69</td>
</tr>
<tr>
<td>View Event Details</td>
<td>70</td>
</tr>
<tr>
<td>View Attribute Changes</td>
<td>74</td>
</tr>
<tr>
<td>View Impacted Domains</td>
<td>78</td>
</tr>
<tr>
<td>Retrieve an Attribute from the List</td>
<td>80</td>
</tr>
<tr>
<td>Trail Flow Use Cases</td>
<td>82</td>
</tr>
<tr>
<td>Indicators of Attack</td>
<td>88</td>
</tr>
<tr>
<td>View Indicators-of-Attack</td>
<td>99</td>
</tr>
<tr>
<td>Understand IoA Security Levels</td>
<td>104</td>
</tr>
<tr>
<td>Timeline Information</td>
<td>105</td>
</tr>
<tr>
<td>IoA Tile Information</td>
<td>108</td>
</tr>
<tr>
<td>Filter Indicators-of-Attack</td>
<td>110</td>
</tr>
<tr>
<td>IoA List of Incidents</td>
<td>117</td>
</tr>
<tr>
<td>Filter Incidents</td>
<td>119</td>
</tr>
<tr>
<td>Incident Details</td>
<td>121</td>
</tr>
<tr>
<td>Close or Reopen Incidents</td>
<td>127</td>
</tr>
<tr>
<td>Understand Attack Details</td>
<td>131</td>
</tr>
<tr>
<td>Export an Attack Report</td>
<td>133</td>
</tr>
<tr>
<td>Export an IoA Report</td>
<td>134</td>
</tr>
<tr>
<td>Use Indicators of Exposure</td>
<td>135</td>
</tr>
<tr>
<td>View Indicators of Exposure</td>
<td>142</td>
</tr>
<tr>
<td>Retrieve an IoE from the List</td>
<td>145</td>
</tr>
<tr>
<td>View Indicator Details</td>
<td>150</td>
</tr>
<tr>
<td>Filter Deviant Objects</td>
<td>158</td>
</tr>
</tbody>
</table>
Retrieve a Deviant Object with the Wizard ................................................................. 159
Retrieve Deviant Object Manually .................................................................................. 166
Ignore a Deviant Object .................................................................................................. 169
View Incriminating Attributes ....................................................................................... 178
Export Deviant Objects Report ....................................................................................... 184

Tenable.ad 3.x User and Administrator Guide Administrator Guide ........................................... 186

Authentication .................................................................................................................. 187
Authentication Using a Tenable.ad Account ........................................................................ 188
Authentication Using LDAP .............................................................................................. 192
Authentication Using SAML ............................................................................................. 195

User Accounts .................................................................................................................. 197
Create a User .................................................................................................................... 198
Edit a User ....................................................................................................................... 200
Deactivate a User .............................................................................................................. 202
Delete a User .................................................................................................................. 203

Security Profiles ............................................................................................................. 204
Create a Security Profile ................................................................................................. 205
Apply a Security Profile to a Workspace ........................................................................ 207
Customize an Indicator ................................................................................................... 208
Refine Customization on an Indicator ............................................................................ 211
Delete a Security Profile ................................................................................................. 213

User Roles ....................................................................................................................... 214
Manage Roles .................................................................................................................. 215
Set Permissions for a Role ............................................................................................... 216
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Permissions on User Interface Entities (Example)</td>
<td>220</td>
</tr>
<tr>
<td>Forests</td>
<td>223</td>
</tr>
<tr>
<td>Domains</td>
<td>224</td>
</tr>
<tr>
<td>Add a Domain</td>
<td>225</td>
</tr>
<tr>
<td>Edit a Domain</td>
<td>227</td>
</tr>
<tr>
<td>Delete a Domain</td>
<td>228</td>
</tr>
<tr>
<td>Force Data Refresh on a Domain</td>
<td>229</td>
</tr>
<tr>
<td>Honey Accounts</td>
<td>230</td>
</tr>
<tr>
<td>Attack Scenarios</td>
<td>233</td>
</tr>
<tr>
<td>Workload Quota</td>
<td>236</td>
</tr>
<tr>
<td>Indicators of Attack and the Active Directory</td>
<td>239</td>
</tr>
<tr>
<td>Credential Dumping: LSASS Memory</td>
<td>241</td>
</tr>
<tr>
<td>DCSHadow</td>
<td>243</td>
</tr>
<tr>
<td>DCSync</td>
<td>244</td>
</tr>
<tr>
<td>Enumeration of Local Administrators</td>
<td>245</td>
</tr>
<tr>
<td>GoldenTicket</td>
<td>248</td>
</tr>
<tr>
<td>Kerberosting</td>
<td>249</td>
</tr>
<tr>
<td>Massive Computers Reconnaissance</td>
<td>251</td>
</tr>
<tr>
<td>NTDS Extraction</td>
<td>255</td>
</tr>
<tr>
<td>Password Guessing</td>
<td>259</td>
</tr>
<tr>
<td>Password Spraying</td>
<td>261</td>
</tr>
<tr>
<td>PetitPotam</td>
<td>263</td>
</tr>
<tr>
<td>SAM Name Impersonation</td>
<td>265</td>
</tr>
<tr>
<td>Alerts</td>
<td>269</td>
</tr>
</tbody>
</table>
SMTP Server Configuration ................................................................. 270
Email Alerts ....................................................................................... 271
Syslog Alerts .................................................................................... 275
Syslog and Email Alert Details ......................................................... 278
Update Your License ......................................................................... 283
Welcome to Tenable.ad

Last updated: 3/11/2022

Tenable.ad allows you to secure your infrastructure by anticipating threats, detecting breaches, and responding to incidents and attacks. Using an intuitive dashboard to monitor your active directory in real-time, you can identify at a glance the most critical vulnerabilities and their recommended courses of remediation. Tenable.ad’s indicators of attack and indicators of exposure allow you to discover underlying issues affecting your active directory, identify dangerous trust relationships, and analyze in-depth details of attacks.

The Indicators of Attack and Indicators of Exposure features are available depending on the license that you purchased.

To get started, see Get Started With Tenable.ad.
Get Started with Tenable.ad 3.x User and Administrator Guide

Use the following getting started sequence to begin working with your Tenable.ad solution.

1. **Prepare**
2. **Configure**
3. **Visualize**
4. **Monitor**
5. **Detect**
6. **Secure**

**Prepare**

- [Connect and sign in](#) to Tenable.ad 3.x User and Administrator Guide
- [Set profile preferences:](#) language, profile, password
- [Learn to navigate the user interface](#)

**Configure**

Dashboards and widgets allow you to view and monitor efficiently the security in your active directory infrastructure.

- [Create dashboards](#)
- [Add widgets](#)

**Visualize the Active Directory**

The **topology graph** displays forests, domains, and the trust relationships that exist between them.

- Filter forests and domains
- [Display trust relationships](#)
- [Investigate dangerous trusts](#)
Monitor

The **trail flow** displays the real-time monitoring and analysis of events affecting your active directory infrastructure.

- View the trail flow in real-time
- Filter real-time events
- Examine event details

Detect

Tenable.ad's **Indicators of attack** help your organization detect and take immediate action to prevent attempts to compromise your AD infrastructures.

- View indicators of attack
- View incident details and attack details

Secure

Tenable.ad's **indicators of exposure** help you detect attack vectors, security gaps, and mis-configurations in your active directory infrastructures before attackers do.

- View indicators of exposure
- Examine indicator details
- Explore deviant objects
Connection to Tenable.ad

You access Tenable.ad's web application through a client URL.

To sign in to Tenable.ad:

1. In any browser, type your client URL (for example: client.tenable.ad) in the address bar.
   
   The Log in window appears.

2. Click one of the following tabs to select your authentication method:
   
   - Using a Tenable.ad account
   - Using an LDAP account
   - Using SAML

Using a Tenable.ad account

To sign in with your Tenable.ad account:

1. Click the Tenable.ad tab.

2. Type your email address.

3. Type your password.

4. Click Log in.

   The Tenable.ad 3.x User and Administrator Guide page opens.

Using an LDAP account

To sign in with LDAP:

1. Click the LDAP tab.

2. Type your LDAP account name.

3. Type your LDAP password.

4. Click Log in.

   The Tenable.ad 3.x User and Administrator Guide page opens.
Using SAML

To sign in with SAML:

1. Click the **SAML** tab.
2. Type your email address.
3. Type your password.
   
   Tenable.ad redirects you to your SAML server for authentication.

4. Click **Log in**.

   The Tenable.ad 3.x User and Administrator Guide page opens.

Caution: If you repeatedly fail to log in, Tenable.ad 3.x User and Administrator Guide locks your account. Contact your administrator.

To sign out of Tenable.ad 3.x User and Administrator Guide:

1. In Tenable.ad 3.x User and Administrator Guide, under **My Settings** in the side navigation bar, click the **icon**.
   
   A submenu appears.

2. Click **Logout**.

   Tenable.ad returns to the Log in page.
User Preferences

You can set your user preferences in Tenable.ad 3.x User and Administrator Guide

- To select your language:
- To select your profile:
- To change your password:
- To select your profile:

To set your preferences:

1. In Tenable.ad, under My Settings in the side navigation bar, click the icon at the bottom.
   A submenu appears.
2. Select Preferences.
   The Preferences pane appears.

To select your language:

a. In Languages, click the arrow of the drop-down list to select your preferred language.
b. Click Save.
   A message confirms that Tenable.ad 3.x User and Administrator Guide updated your preferences. The user interface displays the language you selected.

To select your profile:

Profiles allow you to create and customize your own view of risks affecting your Active Directory:

Each profile displays exposure and attack scenarios specifically configured for users with that profile. For instance, an IT administrator’s general view of the data analysis can be different from that of the Security team, which displays a comprehensive view of all the risks that AD infrastructures face.

a. Under Preferences, click Profiles.

b. In Preferred profile, click the drop-down arrow to select your default profile after you connect to Tenable.ad 3.x User and Administrator Guide.
c. Click **Save**.

A message confirms that Tenable.ad 3.x User and Administrator Guide updated your preferences.

For more information, see [Security Profiles](#).

To change your password:

a. Under **Preferences**, click **Credentials**.

b. Provide the following:
   - Your old password.
   - Your new password.

c. In the **New password confirmation** box, retype the new password.

d. Click **Save**.

A message confirms that Tenable.ad 3.x User and Administrator Guide changed your password.

**Note:** You cannot change a password for accounts connected through external providers such as LDAP or SAML in Tenable.ad.

To manage your API key:

a. Under **Preferences**, click **API key**.

   Your access token appears in the **Current API key** box.

b. You can do the following:

c. Click the **_Copy** icon to copy the API key to the clipboard to use as needed.

d. Click **Refresh API key** to generate a new access token.

   A message asks you for confirmation.

   **Note:** Refreshing the API key causes Tenable.ad 3.x User and Administrator Guide to deactivate the current token.

For more details, see Use Public API.
After you log in to Tenable.ad 3.x User and Administrator Guide, the home page opens, as shown in this example.

<table>
<thead>
<tr>
<th>#</th>
<th>What it is</th>
<th>What it does</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Dashboards</td>
<td>Dashboards allow you to manage and monitor efficiently and in a visual</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td><strong>way security in an Active Directory infrastructure.</strong></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td><strong>Notifications</strong></td>
<td>A bell icon and badge counts notify you of attack alerts and/or exposure alerts waiting for your acknowledgment.</td>
</tr>
<tr>
<td>3.</td>
<td><strong>Connection</strong></td>
<td>This icon indicates that your AD infrastructure is connected to Tenable.ad 3.x User and Administrator Guide. When your AD is disconnected, this icon becomes red.</td>
</tr>
<tr>
<td>4.</td>
<td><strong>Documentation</strong></td>
<td>Click this icon to display the User and Administrator Guides.</td>
</tr>
<tr>
<td>5.</td>
<td><strong>Security Profiles</strong></td>
<td>Security Profiles allow different types of users to review security analysis from different reporting angles.</td>
</tr>
<tr>
<td>6.</td>
<td><strong>Trail Flow</strong></td>
<td>The Trail Flow shows the real-time monitoring and analysis of events affecting your Active Directory.</td>
</tr>
<tr>
<td>7.</td>
<td><strong>Indicators of Exposure</strong></td>
<td>Tenable.ad 3.x User and Administrator Guide uses Indicators of Exposure (IoEs) to measure the security maturity of your Active Directory and assign severity levels (Critical, High, Medium or Low) to the flow of events that it monitors and analyzes.</td>
</tr>
<tr>
<td>8.</td>
<td><strong>Indicators of Attack</strong></td>
<td>Through Indicators of Attack, Tenable.ad 3.x User and Administrator Guide can detect attacks in real-time.</td>
</tr>
</tbody>
</table>
9. **Topology**

The Topology page gives an interactive graph visualization of your Active Directory. It displays the forests, domains and trust relationships that exist between them.

10. **Attack Path**

The Attack Path pages gives graphical representations of Active Directory relationships:

- **Blast Radius**: Evaluates lateral movements in the AD from a potentially compromised asset.
- **Attack Path**: Anticipates privilege escalation techniques to reach an asset from a specific entry point.
- **Asset Exposure**: Measures an asset's vulnerability using asset exposure visualization and tackles all escalation paths.

11. **Management**

**Required User Role**: Organizational User with appropriate permissions.

This section allows you to configure the following:

- **Accounts**: User accounts, roles, and security profiles.
- **System**: Forests and domains, application services, alerts, and authentication.

For more information, see the Tenable.ad 3.x User and Administrator Guide Administrator Guide.
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>12.</td>
<td><strong>User Preferences</strong></td>
<td>This page allows you to configure your language, profile, and password.</td>
</tr>
<tr>
<td>13.</td>
<td>Log out</td>
<td>Click to log out of Tenable.ad 3.x User and Administrator Guide.</td>
</tr>
<tr>
<td>14.</td>
<td><strong>Widgets</strong></td>
<td>Widgets are customizable datasets that a dashboard displays. They can contain bar charts, line charts, and counters.</td>
</tr>
</tbody>
</table>
Notifications

At the top right of the Tenable.ad 3.x User and Administrator Guide home page, a bell icon and its badge counts notify you of attack alerts and/or exposure alerts waiting for your acknowledgment. When it receives new alerts, Tenable.ad 3.x User and Administrator Guide increments the notification badge counts.

<table>
<thead>
<tr>
<th>Blue</th>
<th>Exposure alerts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td>Attack alerts</td>
</tr>
</tbody>
</table>

To display alerts:

1. In Tenable.ad 3.x User and Administrator Guide, click the bell icon.
   
The Alerts pane opens.

2. Do one of the following:
   
   - Click on the Exposure alerts tab to display exposure alerts.
   - Click on the Attack alerts tab to display attack alerts.
   
   A list of associated alerts appears.

To view the event associated with the alert:

1. Select an alert from the list and click Actions> See the deviance.
   
The Event details pane opens with the following information:
   
   - Source (Event collector)
   - Object type
   - File
   - Path
   - Impacted domains
Date
- A list of attributes with values at the time of event and the current value

2. Click the Deviances tab.

The Deviances pane opens with a list of deviances associated with the event.

3. Click on n/n Indicators to display the pane for the Indicator of Exposure that triggered the alert.

4. Click on n/n Reasons to display the reasons for the alert.

5. Click on the arrow to expand or collapse the information for the alert.

6. Click on the Indicator name to display the Indicator details page.

To archive the alert:

After you view the alert, you can archive it.
1. In the list of alerts in the **Alerts** pane, select the checkbox for the alert that you want to archive.
   - Optionally, you can click the checkbox for **n/n objects selected** at the bottom of the pane to select all alerts in bulk.

2. At the bottom of the pane, click **Select an action > Archive**.

3. Click **OK**.
Dashboards

Dashboards allow you to visualize data and trends affecting the security of your Active Directory. You can customize them with widgets to display charts and counters according to your requirements.

To create a new dashboard:

1. In Tenable.ad 3.x User and Administrator Guide, click **Dashboards**.
2. Click **Add > Add a dashboard** at the top right corner.
   
The **Add a dashboard** pane opens.
3. In the **Name** box, type a name for the dashboard.
4. Click **OK**.
   
   A message confirms that Tenable.ad 3.x User and Administrator Guide created the dashboard. The new dashboard has a tab under **Dashboards**.

To rename a dashboard:

1. In Tenable.ad 3.x User and Administrator Guide, click **Dashboards**.
2. Select the tab for the dashboard that you want to rename.
3. Click **Configure > Configure the dashboard** at the top right corner.
   
The **Configure the dashboard** pane opens.
4. In the **Name** box, type another name for the dashboard.
5. Click **OK**.
   
   A message confirms that Tenable.ad 3.x User and Administrator Guide updated the dashboard.

To delete a dashboard:

1. In Tenable.ad 3.x User and Administrator Guide, click **Dashboards**.
2. Select the tab for the dashboard that you want to delete.
3. Click **Configure > Delete the dashboard** at the top right corner.

   The **Delete the dashboard** pane opens and asks you to confirm the deletion.

4. Click **Delete**.

   A message confirms that Tenable.ad 3.x User and Administrator Guide deleted the dashboard.
Widgets

Widgets in dashboards allow you to visualize your Active Directory data in the form of bar charts, line charts, and counters. You can customize widgets to display specific information and drag them around to reposition them on the dashboard.

You can add widgets to a newly created dashboard or an existing dashboard.

To add a widget to a dashboard:

1. In Tenable.ad 3.x User and Administrator Guide, click **Dashboards**.

2. Do one of the following:
   - On a new dashboard, click **Add a widget on this dashboard**.
   - On an existing dashboard, click **Add > Add a widget on this dashboard** at the top right corner.

The **Add a widget** pane opens.
3. Under **Main Information**, click on a tile to select one of the following:
   - Bar chart:
   - Line chart
   - Counter

4. In the **Name of the widget** box, type a name for the widget

5. Under **Widget Configuration**, in the **Type of data** box, click the arrow on the drop-down list to select one of the following:
   - Users count: The number of active users for the domain.
   - Deviances count: The number of deviances or security breaches detected.
   - Compliance score: A score of 0-100 that Tenable.ad 3.x User and Administrator Guide computes by taking into account the number of deviances detected and their severity levels.
   - Duration (for line chart): Click the arrow on the drop-down list to select the duration to display.
6. Under **Datasets Configuration**:

<table>
<thead>
<tr>
<th>Datasets Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status</strong> (User count)</td>
</tr>
</tbody>
</table>
| **Indicators**          | a. Click **Indicators** to select the indicator(s). The **Indicators of Exposure** pane opens.  
                          | b. Select an indicator or indicators from the list. Optionally, you can also:  
                          |   ▪ Type an indicator name in the Search box.  
                          |   ▪ Select all indicators.  
                          |   ▪ Select all indicators of a specific severity level (critical, high, medium, or low).  
                          | c. Click **Filter on selection**. |
| **Domains**             | a. Click **Domains** to select the domain(s). The **Forests and Domains** pane opens.  
                          | b. Select a domain from the list. Optionally, you can also:  
                          |   ▪ Type a domain name in the Search box.  
                          |   ▪ Select all domains.  
                          | c. Click **Filter on selection**. |

7. In the Name of the dataset box, type a name for the dataset. The **Forests and Domains** pane opens.

8. Select the domain for the widget. Optionally, you can type a domain name in the Search box.

9. Click **Filter on selection**.

---

Copyright © 2022 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.
10. Optionally, you can click on **Add a new dataset** to add another dataset with different options for the widget.

11. Click **Add**.

   A message confirms that Tenable.ad 3.x User and Administrator Guide added the widget.

**To modify a widget:**

1. In Tenable.ad 3.x User and Administrator Guide, click **Dashboards**.

2. Select the dashboard that contains the widget you want to modify.

3. Select the widget.

4. Click the 🔄 icon at the widget's top right corner.

   The **Modify a widget** pane opens.

5. Make the necessary modifications.

6. Click **Edit**.

   A message confirms that Tenable.ad 3.x User and Administrator Guide updated the widget.

**To refresh a widget:**

1. Select the widget.

2. Click the ⏰ icon at the widget's top right corner.

   The widget refreshes.

**To delete a widget:**

1. In Tenable.ad 3.x User and Administrator Guide, click **Dashboards**.

2. Select the dashboard that contains the widget you want to delete.

3. Select the widget.

4. Click the 🗑️ icon.

   The Remove a widget pane opens. A message asks you to confirm the deletion.

5. Click **OK**.
A message confirms that Tenable.ad 3.x User and Administrator Guide deleted the widget from the dashboard.
Topography

The Topology page provides an interactive graphic visualization of your Active Directory. The **Topo-logy Graph** displays the forests, domains and trust relationships that exist between them.

![Topology Graph](image)

**To open the Topology page:**

- In Tenable.ad 3.x User and Administrator Guide, click on **Topology** on the left navigation menu.

    The Topology pane opens with a graphical representation of your AD.

**To search for a domain:**

- In the **Topology** pane, type a domain name in the **Search** box.

    Tenable.ad 3.x User and Administrator Guide highlights the domain.

**To zoom in on the graph:**
In the **Topology** pane, click on the **Zoom** slider to adjust the graph size.

To display the link between two domains:

- In the **Topology** pane, click the **Show internal relationships** toggle to **Yes**.

To display details about a domain:

- In the **Topology** pane, click on the ▲ for the domain name.

The **Domain details** pane opens with the Indicators of Exposure (IoE) detected and the compliance score for the domain. You can click on the tile for the IoE to drill down for more information.
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.
Trust Relationships

The curved arrows between domains on the topology graph represent trust relationships.

To display trust relationships:

- On the topology graph, hover over the curved arrows.

  Tenable.ad 3.x User and Administrator Guide displays the trust relationships display specific attributes between two entities.

The trust attribute information indicates the trust direction as **unidirectional** or **bidirectional** (incoming/outgoing) and displays one of the following values:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-transitive</td>
<td>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.</td>
</tr>
<tr>
<td>Forest transitive</td>
<td>Indicates that a transitive trust exists between two forests. The trust granted to another domain can pass to the trusted forest.</td>
</tr>
<tr>
<td><strong>Within forest</strong></td>
<td>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 <strong>QuarantinedWithinForest</strong>.</td>
</tr>
<tr>
<td><strong>Uplevel only</strong></td>
<td>Indicates that only clients running Windows 2000 operating systems and later can use this trust.</td>
</tr>
<tr>
<td><strong>Treat as external</strong></td>
<td>(Only when FOREST_TRANSITIVE is set) Indicates an external type of trust. Tenable.ad 3.x User and Administrator Guide modifies the security identifier (SID) filtering on the trust and authorizes the SIDs whose relative identifier (RID) is greater than or equal to 1000 to pass across the forest.</td>
</tr>
<tr>
<td><strong>Quarantined</strong></td>
<td>Indicates that Tenable.ad 3.x User and Administrator Guide enabled the filtering of the SIDs whose RID is greater than or equal to 1000 for the trust. By default, Tenable.ad 3.x User and Administrator Guide only enables it for an external trust but it can also apply to a parent-child trust or a forest trust.</td>
</tr>
<tr>
<td><strong>Cross-organization authentication</strong></td>
<td>Indicates that Tenable.ad 3.x User and Administrator Guide enabled selective authentication and can use it across domain or forest trusts.</td>
</tr>
<tr>
<td><strong>Selective authentication</strong></td>
<td>See Cross-organization authentication.</td>
</tr>
<tr>
<td><strong>Cross-organization without TGT delegation</strong></td>
<td>Displays if the delegation on a trusted domain is fully disabled (never sets the ok-as-delegate option in the issued service tickets).</td>
</tr>
<tr>
<td><strong>RC4 encryption:</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>AES keys</strong></td>
<td>Indicates that the trust supports AES-encryption keys for Kerberos exchanges.</td>
</tr>
<tr>
<td><strong>PIM trust</strong></td>
<td>If the FOREST_TRANSITIVE and TREAT_AS_EXTERNAL flags are set and</td>
</tr>
</tbody>
</table>
the QUARANTINED_DOMAIN flag is not 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.

| No attribute | Indicates that the external trust has no specific attribute. |

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

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

To investigate a dangerous trust:

- On the topology graph, click on the curved arrows.

  The **Deviant objects related to trusts** opens.
Dangerous Trusts

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

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

To investigate a dangerous trust:

1. On the topology graph, click on the curved arrows.

   The **Deviant objects related to trusts** opens.

   **Tip**: The details of the events displayed on this dangerous trust relationships pane are all linked to the **Dangerous Trust Relationship** Indicator of Exposure which you can also access from the **Indicators of Exposure** navigation menu.

   ![Topology Graph with Deviant Objects](image)

2. Hover over and click on a deviant object from the list to display the details.
Trail Flow

Using the trail flow, Tenable.ad 3.x User and Administrator Guide continuously monitors your infrastructure and detects regressions as they happen.

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

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

The **Trail Flow** page allows you to load previous events and 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.
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.
<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>nTDSlsa</td>
<td>computer</td>
<td>CN</td>
<td>Tenable's dom</td>
<td>06-24</td>
</tr>
<tr>
<td>LDAP</td>
<td>SPN change</td>
<td>computer</td>
<td>CN</td>
<td>Tenable's dom</td>
<td>06-24</td>
</tr>
<tr>
<td>LDAP</td>
<td>Object deleted</td>
<td>server</td>
<td>CN</td>
<td>Tenable's dom</td>
<td>06-24</td>
</tr>
<tr>
<td>LDAP</td>
<td>Object deleted</td>
<td>nTDSlsa</td>
<td>CN</td>
<td>Tenable's dom</td>
<td>06-24</td>
</tr>
<tr>
<td>LDAP</td>
<td>New object</td>
<td>nTDSlsa</td>
<td>CN</td>
<td>Tenable's dom</td>
<td>06-24</td>
</tr>
<tr>
<td>LDAP</td>
<td>New object</td>
<td>server</td>
<td>CN</td>
<td>Tenable's dom</td>
<td>06-24</td>
</tr>
<tr>
<td>LDAP</td>
<td>SPN change</td>
<td>computer</td>
<td>CN</td>
<td>Tenable's dom</td>
<td>06-24</td>
</tr>
<tr>
<td>LDAP</td>
<td>SPN change</td>
<td>computer</td>
<td>CN</td>
<td>Tenable's dom</td>
<td>06-24</td>
</tr>
<tr>
<td>LDAP</td>
<td>SPN change</td>
<td>computer</td>
<td>CN</td>
<td>Tenable's dom</td>
<td>06-24</td>
</tr>
<tr>
<td>LDAP</td>
<td>SPN change</td>
<td>computer</td>
<td>CN</td>
<td>Tenable's dom</td>
<td>06-24</td>
</tr>
<tr>
<td>LDAP</td>
<td>SPN change</td>
<td>computer</td>
<td>CN</td>
<td>Tenable's dom</td>
<td>06-24</td>
</tr>
<tr>
<td>LDAP</td>
<td>Failed authentic user</td>
<td>CN</td>
<td>Tenable's dom</td>
<td>06-24</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>SPN change</td>
<td>computer</td>
<td>CN</td>
<td>Tenable's dom</td>
<td>06-24</td>
</tr>
<tr>
<td>LDAP</td>
<td>Object deleted</td>
<td>server</td>
<td>CN</td>
<td>Tenable's dom</td>
<td>06-24</td>
</tr>
<tr>
<td>LDAP</td>
<td>Object deleted</td>
<td>nTDSlsa</td>
<td>CN</td>
<td>Tenable's dom</td>
<td>06-24</td>
</tr>
<tr>
<td>LDAP</td>
<td>New object</td>
<td>nTDSlsa</td>
<td>CN</td>
<td>Tenable's dom</td>
<td>06-24</td>
</tr>
<tr>
<td>LDAP</td>
<td>New object</td>
<td>server</td>
<td>CN</td>
<td>Tenable's dom</td>
<td>06-24</td>
</tr>
<tr>
<td>LDAP</td>
<td>nTDSlsa</td>
<td>CN</td>
<td>Tenable's dom</td>
<td>06-24</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN</td>
<td>Tenable's dom</td>
<td>06-24</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN</td>
<td>Tenable's dom</td>
<td>06-24</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN</td>
<td>Tenable's dom</td>
<td>06-24</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN</td>
<td>Tenable's dom</td>
<td>06-24</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN</td>
<td>Tenable's dom</td>
<td>06-24</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN</td>
<td>Tenable's dom</td>
<td>06-24</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>user</td>
<td>CN</td>
<td>Tenable's dom</td>
<td>06-24</td>
<td></td>
</tr>
</tbody>
</table>
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.
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.
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 ❶ 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 ❷ 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 ❸ under the attribute fields.

Query syntax

Add an attribute

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

2. Click on the +Add a new rule action button ❶ 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 ❶.

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.

![Search Wizard interface with query expression]

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.
### Trail Flow

```plaintext
<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>SYSVOL</td>
<td>ACL change</td>
<td>Folder</td>
<td></td>
<td>Tenable's doma</td>
<td>16:24:40, 2021-06-29</td>
</tr>
<tr>
<td>SYSVOL</td>
<td>ACL change</td>
<td>Folder</td>
<td></td>
<td>Tenable's doma</td>
<td>16:24:40, 2021-06-29</td>
</tr>
<tr>
<td>SYSVOL</td>
<td>ACL change</td>
<td>Folder</td>
<td></td>
<td>Tenable's doma</td>
<td>16:24:40, 2021-06-29</td>
</tr>
<tr>
<td>SYSVOL</td>
<td>ACL change</td>
<td>Folder</td>
<td></td>
<td>Tenable's doma</td>
<td>16:24:40, 2021-06-29</td>
</tr>
<tr>
<td>SYSVOL</td>
<td>ACL change</td>
<td>Folder</td>
<td></td>
<td>Tenable's doma</td>
<td>16:24:40, 2021-06-29</td>
</tr>
<tr>
<td>SYSVOL</td>
<td>ACL change</td>
<td>Folder</td>
<td></td>
<td>Tenable's doma</td>
<td>16:24:40, 2021-06-29</td>
</tr>
<tr>
<td>SYSVOL</td>
<td>ACL change</td>
<td>Folder</td>
<td></td>
<td>Tenable's doma</td>
<td>16:24:40, 2021-06-29</td>
</tr>
<tr>
<td>SYSVOL</td>
<td>ACL change</td>
<td>Folder</td>
<td></td>
<td>Tenable's doma</td>
<td>16:24:40, 2021-06-29</td>
</tr>
<tr>
<td>SYSVOL</td>
<td>ACL change</td>
<td>Folder</td>
<td></td>
<td>Tenable's doma</td>
<td>16:24:40, 2021-06-29</td>
</tr>
<tr>
<td>SYSVOL</td>
<td>ACL change</td>
<td>Folder</td>
<td></td>
<td>Tenable's doma</td>
<td>16:24:40, 2021-06-29</td>
</tr>
<tr>
<td>SYSVOL</td>
<td>ACL change</td>
<td>Folder</td>
<td></td>
<td>Tenable's doma</td>
<td>16:24:40, 2021-06-29</td>
</tr>
<tr>
<td>SYSVOL</td>
<td>ACL change</td>
<td>Folder</td>
<td></td>
<td>Tenable's doma</td>
<td>16:24:40, 2021-06-29</td>
</tr>
<tr>
<td>SYSVOL</td>
<td>ACL change</td>
<td>Folder</td>
<td></td>
<td>Tenable's doma</td>
<td>16:24:40, 2021-06-29</td>
</tr>
<tr>
<td>SYSVOL</td>
<td>ACL change</td>
<td>Folder</td>
<td></td>
<td>Tenable's doma</td>
<td>16:24:40, 2021-06-29</td>
</tr>
<tr>
<td>SYSVOL</td>
<td>ACL change</td>
<td>Folder</td>
<td></td>
<td>Tenable's doma</td>
<td>16:24:40, 2021-06-29</td>
</tr>
<tr>
<td>SYSVOL</td>
<td>ACL change</td>
<td>Folder</td>
<td></td>
<td>Tenable's doma</td>
<td>16:24:40, 2021-06-29</td>
</tr>
<tr>
<td>SYSVOL</td>
<td>ACL change</td>
<td>Folder</td>
<td></td>
<td>Tenable's doma</td>
<td>16:24:40, 2021-06-29</td>
</tr>
<tr>
<td>SYSVOL</td>
<td>ACL change</td>
<td>Folder</td>
<td></td>
<td>Tenable's doma</td>
<td>16:24:40, 2021-06-29</td>
</tr>
<tr>
<td>SYSVOL</td>
<td>ACL change</td>
<td>Folder</td>
<td></td>
<td>Tenable's doma</td>
<td>16:24:40, 2021-06-29</td>
</tr>
<tr>
<td>SYSVOL</td>
<td>ACL change</td>
<td>Folder</td>
<td></td>
<td>Tenable's doma</td>
<td>16:24:40, 2021-06-29</td>
</tr>
</tbody>
</table>
```

### EDIT QUERY EXPRESSION

**Filter preview**: `isdeviant: true AND globalpath: "sysvol"`

**AND** or **OR** options:

- **AND**
- **OR**
- **Deviant only**

**globalpath** field:

- Add a new rule: `/ Add a new condition: AND OR`

**sysvol** field

- **Cancel**
- **Reset**
- **Validate**
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.

![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-
Load Previous Events

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 on the right of the pane and select the folder to be looked in.
- To edit a bookmark name, click on the Pencil icon.
- To delete an expression from the Bookmarks blade, select the Bin icon.
- To edit a bookmark folder name (if any), click on the Pencil icon.
- To delete a bookmark folder (if any), select the Bin icon.
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>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute</td>
<td>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.</td>
</tr>
<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

ATTACKER KNOWN TOOLS

- mimikatz
- Gentil Kini
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.

![Active Directory Users and Computers](image-url)
On the end-user’s side, the **Trail Flow** page is updated. Take a look at the **Type** column which indicates *New object*.

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](#).
Indicators of Attack

The **Indicators of Attack** feature gives your organization the ability to detect attacks in real time and quickly stop them by:

- Visualizing every threat from an accurate attack timeline.
- Consolidating attack distribution in a single view.
- Analyzing in-depth details about an AD attack.
- Exploring 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 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 ❶ for the tiles:

- Alphabetical order
- Criticality
- Forest

For more details on tile sorting, see View 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 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:
Tile sorting order

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 Indicators-of-Attack.
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 ❶.
- Access detailed explanations on the attacks affecting AD infrastructures ❷.
- Close or reopen an incident ❸.
- Download a report showing all incidents ❹.

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.

Open/close incidents
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

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.
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.
• 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
View Indicator Details

Tenable.ad provides detailed information on each Indicator of Exposure affecting your AD infrastructures. 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.
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.

![Image of Tenable.ad blade]

**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.

---

Add a combinator to the first condition in the query
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 🟥 to be applied to the first condition.

3. Select the attribute from the dropdown menu and enter its value 📝. To add an attribute, click on the + Add a new rule action button 🌟.
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

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

You can choose to ignore one or several deviant objects. You can apply a custom filter immediately or to specify a time frame to activate the filter.

**Note:** Ignoring an object does not make it resolved in Tenable.ad 3.x User and Administrator Guide.

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 drop-down 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.

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.

2. Select the Start date and End date from the date picker 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, 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, check the boxes in the upper-right corner.

3. Verify that the Select all box 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 and click OK.

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 or click individually on each reason to be ignored/unignored.

Then, choose the action from the dropdown menu 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.
**DEVIAN OBJECTS**

**NOT PROTECTED AGAINST DELEGATION**

The `admin` account is privileged (C=Administrators, O=Multin, DC=alid, DC=corp), 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 `admin` account and thus benefit from the privileges of this account to perform malicious actions, within the limits of the authorized delegation.
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.
Tenable.ad 3.x User and Administrator Guide Administrator Guide

Last updated: March 11, 2022

The Administrator's Guide provides information about administration tasks for Tenable.ad.

It targets users with permissions to manage the following:

- Authentication
- User Accounts
- Security Profiles
- User Roles
- Forests
- Domains
- Indicators of Attack and the Active Directory
- Alerts
- Update Your License
Authentication

There are three ways to authenticate Tenable.ad 3.x User and Administrator Guide users:

- Authentication Using a Tenable.ad Account
- Authentication Using LDAP
- Authentication Using SAML
Authentication Using a Tenable.ad Account

The simplest authentication method is through a Tenable.ad 3.x User and Administrator Guide account that requires a username and a password.

This authentication method offers a default lockout policy, a security control designed to mitigate brute force attacks against authentication mechanisms. It locks out user accounts after too many failed login attempts. When an account is locked, users do not have access to Tenable.ad APIs.

To configure authentication using a Tenable.ad 3.x User and Administrator Guide account:

1. In Tenable.ad 3.x User and Administrator Guide, click **Systems > Configuration**. The configuration pane appears.
2. Under the **Authentication** section, click **Tenable.ad**.
3. In the **Default profile** drop-down box, select the profile for the user.
4. In the **Default roles** box, select the roles for the user.
5. Configure the lockout policy settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enabled</strong></td>
<td>• <strong>Enabled</strong>— Tenable.ad blocks the account after a set number of failed login attempts.</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>— Tenable.ad does not lock the account after failed login attempts.</td>
<td></td>
</tr>
<tr>
<td><strong>Lockout duration</strong></td>
<td>The time duration that Tenable.ad locks the account from any login attempts. Tenable.ad automatically unlocks the account after this time elapses to allow the user to attempt to log in again.</td>
<td>300 seconds</td>
</tr>
<tr>
<td></td>
<td>To configure the lockout duration:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Click on the slider to set a lockout duration.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Select <strong>Infinite</strong> if you do not want to unlock the account automatically after a set duration.</td>
<td></td>
</tr>
<tr>
<td><strong>Number of attempts before lockout</strong></td>
<td>The number of failed login attempts before Tenable.ad locks the account.</td>
<td>3</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>
<td>900 seconds</td>
</tr>
<tr>
<td></td>
<td>To set the redemption period:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Click on the slider to set a time interval.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Select &quot;Infinite&quot; if you do not want to set a time interval to count unsuccessful login attempts</td>
<td></td>
</tr>
</tbody>
</table>
6. Click **Save**.

**To disable the lockout policy:**

1. In Tenable.ad 3.x User and Administrator Guide, click **Systems > Configuration**. The configuration pane appears.
2. Click the **Enabled** toggle to turn off the lockout policy.

**Note:** If you disable the lockout policy, locked user accounts can attempt to reconnect.

**To view the list of locked accounts:**

- In Tenable.ad, go to **Accounts > User accounts management**.

  In the list of users, Tenable.ad 3.x User and Administrator Guide displays the locked accounts with a red padlock icon. 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."

**To unlock an account:**

You must have permissions to edit users in order to unlock accounts.

1. In Tenable.ad, click **Accounts > User accounts management**. The user accounts management pane appears.
2. In the list of users, locate the locked account.
3. Click the pencil icon to edit the locked user account. The user's information pane appears.
4. Click the **Remove lockout** button.

**To grant permissions to user roles to configure the lockout policy:**
1. In Tenable.ad, click Accounts > Roles management.
   The Roles management pane appears.

2. Click the pencil icon next to a role name to edit the role.
   The Edit a role pane appears.

3. Click the System configuration entities tab.

4. Under the Permissions Management section, select the Accounts Lockout Policy checkbox.

5. Click the toggle to Unauthorized or Granted.

   A message confirms that Tenable.ad 3.x User and Administrator Guide updated the user's permissions.

   **Note:** Tenable.ad 3.x User and Administrator Guide disables the lockout policy settings for users who only have read permission in this pane.
Authentication Using LDAP


To enable LDAP authentication, you must have the following:

- A preconfigured service account with a user and password to access the Active Directory.
- A preconfigured Active Directory group.

After you set up LDAP authentication, the LDAP option appears in a tab on the login page.

To configure LDAP authentication:

1. In Tenable.ad 3.x User and Administrator Guide, click **Systems > Configuration**.
   
   The configuration pane appears

2. Under the **Authentication** section, click **LDAP**.

3. Click the **Enable LDAP authentication** toggle to enabled.
   
   An LDAP information form appears.

4. Provide the following information:

   - In the **Address of the LDAP server** box, type the LDAP server's IP address beginning with `ldap://` and ending with the domain name and port number.

     **Note:** If you use an LDAPS server, type its address beginning with `ldaps://` and ending with the domain name and port number. See the procedure [To add a DER-encoded certificate for LDAPS](#) to complete the configuration for LDAPS.

   - In the **Service account use to query the LDAP server** box, type the Distinguished Name (DN), SamAccountName, or UserPrincipalName that you use to access the LDAP server.

   - In the **Service account password** box, type the password for this service account.

   - In the **LDAP search base** box, type the LDAP directory that Tenable.ad 3.x User and Administrator Guide uses to search for users who attempt to connect, beginning with `DC=` or `OU=`. This can be a root directory or a specific organizational unit.
In the **LDAP search filter** box, type the attribute that Tenable.ad 3.x User and Administrator Guide uses to filter users. A standard attribute for authentication in Active Directory is `sAMAccountName={{login}}`. The value for `login` is the value that user provides during authentication.

5. For **Enable SASL bindings**, do one of the following:

   - If you use SamAccountName for the service account, click the **Enable SASL bindings** toggle to enabled.
   - If you use the Distinguished Name or UserPrincipalName for the service account, leave the **Enable SASL bindings** as disabled.

6. Under the **Default Profile and Roles** section, click **Add an LDAP group** to specify the groups allowed to authenticate.

   An LDAP group information form appears.

   - In the **LDAP group name** box, type the distinguished name of the group (example: `CN=TAD_User,OU=Groups,DC=Tenable,DC=ad`)
   - In the **Default profile** drop-down box, select the profile for the allowed group.
   - In the **Default roles** box, select the roles for the allowed group.

7. If necessary, click on the ✪ icon to add a new allowed group.

8. Click **Save**.

To add a DER-encoded certificate for LDAPS:

1. In Tenable.ad 3.x User and Administrator Guide, click **Systems**.

2. Click the **Configuration** tab to display the configuration pane.

3. Under the **Application Services** section, click **PKI Settings**.

4. In the **Additional certificates** box, paste your company’s DER-encoded certificate for Tenable.ad 3.x User and Administrator Guide to use.

5. Click **Save**.

For more information about security profiles and roles, see:
• Security Profiles
• User Roles
Authentication Using SAML

You can configure SAML authentication so that Tenable.ad users can use identity provider-initiated single sign-on (SSO) when logging into Tenable.ad.

Before you begin:

Check that you have the following for the identity provider (IDP):

- SAML v2 only.
- "Assertion encryption" enabled.
- IDP groups that Tenable.ad 3.x User and Administrator Guide uses to grant access to in the Tenable.ad 3.x User and Administrator Guide web portal.
- URL of the SAML server.
- Certificate of the SAML server in DER-ENCODED format, beginning with -----BEGIN CERTIFICATE REQUEST----- and ending with -----END CERTIFICATE REQUEST-----.

To configure SAML authentication:

1. In Tenable.ad 3.x User and Administrator Guide, click **Systems > Configuration**.
   
The configuration pane appears.

2. Under the **Authentication** section, click **SAML Single Sign-on**.

3. Click the **Enable SAML authentication** toggle.
   
   A SAML information form appears.

4. Provide the following information:
   
   - In the **URL of the SAML server** box, type the full URL of the IDP's SAML server where Tenable.ad must connect.
   
   - In the **PKI Settings** box, paste the SAML server certificate from the SAML server.
5. Click **Download** to download the Tenable.ad certificate to use in the SAML server.

6. Click the **Activate automatically new user's account** toggle to activate new user accounts after the first SAML login.

7. Under the **Default Profile and Roles** section, click **Add a SAML group** to specify the groups allowed to authenticate.

   A SAML group information form appears.

8. Provide the following information:
   - In the **SAML group name** box, type the name of the allowed group as it appears in the SAML server.
   - In the **Default profile** drop-down box, select the profile for the allowed group.
   - In the **Default roles** box, select the roles for the allowed group.

9. If necessary, click on the + icon to add a new allowed group.

10. Click **Save**.

    After you set up SAML authentication, the SAML option appears in a tab on the login page.

For more information about security profiles and roles, see:

- **Security Profiles**
- **User Roles**
User Accounts

The **Users Accounts Management** page provides the ability to add, edit, delete, or view the details of Tenable.ad user accounts.

Users belongs to two categories:

- **Global Administrator** – An administrator role that includes all permissions.
- **User** – A simple user role with read-only permissions over business data only.

For more information, see:

- [Create a User](#)
- [Edit a User](#)
- [Deactivate a User](#)
- [Delete a User](#)
Create a User

Required User Role: Administrator or organizational user with appropriate permissions.

To create a user:

1. In Tenable.ad, click Accounts > User accounts management.
   The User accounts management pane appears.

2. Click the Create a user button on the right.
   The Create a user pane appears.

3. Under the Main Information section, type the following information about the user:
   - First name
   - Surname (last name)
   - Email
   - Password: requires at least 8 characters
   - Password confirmation
   - Department
   - Biography

4. Click the toggle Allow authentication to activate the user.

5. Under the Roles Management section, select a role to apply to the user.

6. Click Create.
   A message confirms that Tenable.ad 3.x User and Administrator Guide created the user with the selected role.

See also
- Edit a User
- Deactivate a User
- Delete a User
Edit a User

**Required User Role:** Administrator or organizational user with appropriate permissions.

To edit a user:

1. In Tenable.ad, click Accounts > User accounts management.

   The **User accounts management** pane appears.

2. In the list of users, hover over the line where the user’s name appears and click the ✎ icon at the end of the line.

   The **Edit a user** pane appears.

3. Under the **Main Information** section, modify the information about the user as needed:
   - First name
   - Surname (last name)
   - Email
   - Password: requires at least 8 characters
   - Password confirmation
   - Department
   - Biography

4. Under the **Roles Management** section, modify the user’s role as needed.

5. Click **Edit**.

   A message confirms that Tenable.ad 3.x User and Administrator Guide updated the user with the selected role.

See also
• Create a User

• Deactivate a User

• Delete a User
Deactivate a User

**Required User Role:** Administrator or organizational user with appropriate permissions.

To deactivate a user:

1. In Tenable.ad, click Accounts > User accounts management.
   
   The User accounts management pane appears.

2. In the list of users, hover over the line where the user’s name appears and click the edit icon at the end of the line.

   The Edit a user pane appears.

3. Click the toggle Allow authentication to deactivate the user.

4. Click Edit.

   A message confirms that Tenable.ad 3.x User and Administrator Guide updated the user.

See also

- [Create a User](#)
- [Edit a User](#)
- [Delete a User](#)
Delete a User

**Required User Role:** Administrator or organizational user with appropriate permissions.

To delete a user:

1. In Tenable.ad, click **Accounts > User accounts management**.
   
   The **User accounts management** pane appears.

2. In the list of users, hover over the line where the name of the user you want to delete appears and click the ⌒ icon at the end of the line.

   A message asks you to confirm the deletion.

3. Click **Delete**.

   A message confirms that Tenable.ad 3.x User and Administrator Guide deleted the user.

See also

- [Create a User](#)
- [Edit a User](#)
- [Deactivate a User](#)
Security Profiles

The Security Profiles Management pane allows you to maintain different types of users who can review security analysis from different reporting angles. Security profiles also allow you to customize the behavior of indicators of exposure and indicators of attack.

For more information, see:

- [Create a Security Profile](#)
- [Delete a Security Profile](#)
- [Customize an Indicator](#)
- [Refine Customization on an Indicator](#)
- [Apply a Security Profile to a Workspace](#)
Create a Security Profile

**Required User Role:** Administrator or organizational user with appropriate permissions.

To create a new security profile:

1. In Tenable.ad, click **Accounts > Security profiles management**.
   
   The **Security profiles management** pane appears.

2. Click the **Create a profile** button on the right.
   
   The **Create a profile** pane appears.

3. From the Action drop-down box, you can either:
   
   - **Create a new profile**.
   
   - **Copy** an existing security profile from which you can create a new profile.

4. In the **Name of the new profile** box, type a name for the new profile.
   
   **Note:** Tenable.ad 3.x User and Administrator Guide only accepts alphanumeric characters and underscores.

5. Click the **Create** button in the lower-right corner.
   
   A message indicates that Tenable.ad 3.x User and Administrator Guide created the profile.

   The **Profile Configuration** pane appears.

What to do next

To complete the profile creation, see **Customize an Indicator** for more information.

See also

- **Delete a Security Profile**
- **Customize an Indicator**
- **Refine Customization on an Indicator**
- **Apply a Security Profile to a Workspace**
Apply a Security Profile to a Workspace

**Required User Role:** Administrator or organizational user with appropriate permissions.

Applying a security profile to a workspace allows different types of users to review the data analysis from different reporting angles, as defined by the indicators for that security profile.

Switching from one security profile to another changes the way Tenable.ad 3.x User and Administrator Guide displays the configuration of indicators and the data representation on the dashboards, widgets, and trail flow.

To apply a security profile to a workspace:

1. In Tenable.ad 3.x User and Administrator Guide, click the arrow in the upper-right corner of the window to display a list of available security profiles.

2. Click on the security profile name to select it.

   Tenable.ad 3.x User and Administrator Guide refreshes the dashboard to display data analysis for that security profile.

See also

- [Create a Security Profile](#)
- [Delete a Security Profile](#)
- [Customize an Indicator](#)
- [Refine Customization on an Indicator](#)
Customize an Indicator

**Required User Role:** Administrator or organizational user with appropriate permissions.

You can customize indicators of exposure and indicators of attack for a security profile.

**Note:** You cannot customize the default Tenable.ad security profile. You can only view and copy the Tenable.ad security profile settings. Click on the icon at the end of the line to display the Tenable.ad profile settings.

To customize an indicator:

1. In Tenable.ad, click **Accounts > Security profiles management**.
   The **Security profiles management** pane appears.

2. In the list of security profiles, hover over the security profile that contains the indicator you want to customize. Click on the icon at the end of the line where the security profile file name appears.
   The **Profile configuration** pane appears.

3. Select the tab for **Indicators of Exposure** or **Indicators of Attack**.

4. (Optional) In the **Search an indicator** box, type an indicator name.

5. Click the name of the an indicator to customize.
   The **Indicator Customization** pane appears.

6. Make the necessary customization to the indicator.

**Note:** Certain indicator options require the use of regular expressions (regex). Regex are a 'contain' match instead of an 'equal' match. Example: When you provide "admin" as the input option, you can whitelist a user with "samAccountName=admin" as well as a user with "samAccountName=admintoto".

- To get an exact match, you must use Regex special characters ("^...$") syntax.
- You must also escape special characters with a backslash when using regex. Example: To declare "domain\user" and "CN=Vincent C. (Test),DC-tenable,DC=corp", you type "domain\user" and "CN=Vincent C. \(Test\),DC=tenable,DC=corp".

7. Click **Save as draft**.
A message confirms that Tenable.ad 3.x User and Administrator Guide saved the customization options.

To apply the customization:

1. You can either:
   - In the **Profile configuration** pane, click **Apply pending customization** in the lower-right corner, or
   - In the **Security profiles management** pane, click the ✔ icon at the end of the line where the name of the security profile appears.

   A message appears to warn you that applying the customization erases all its data and requires a complete analysis of the monitored Active Directory, which can take some time.

2. Click **OK**.

   A message confirms that Tenable.ad 3.x User and Administrator Guide applied the customization options. 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.

To discard the customization:

- You can either:
  - In the **Profile configuration** pane, click **Revert pending customization** in the lower-left corner, or
  - In the **Security profiles management** pane, click the ⬅️ icon at the end of the line where the name of the security profile appears.

   A message confirms that Tenable.ad 3.x User and Administrator Guide canceled the customization options.

See also

- [Create a Security Profile](#)
- [Delete a Security Profile](#)
• Refine Customization on an Indicator

• Apply a Security Profile to a Workspace
Refine Customization on an Indicator

Required User Role: Administrator or organizational user with appropriate permissions.

Additional customization on an indicator for a security profile allows you to select indicator options for specific domains. By default, the global customization applies to all domains.

To refine the customization on an indicator:

1. In Tenable.ad, click **Accounts > Security profiles management**.
   The **Security profiles management** pane appears.

2. In the list of security profiles, hover over the security profile that contains the indicator you want to customize. Click on the icon at the end of the line where the security profile file name appears.
   The **Profile configuration** pane appears.

3. Select the tab for **Indicators of Exposure** or **Indicators of Attack**.

4. (Optional) In the **Search an indicator** box, type an indicator name.

5. Click the name of the an indicator to customize.
   The **Indicator Customization** pane appears.

6. Next to the **Global customization** tab, click the icon.
   A **Customization No. 1** tab appears.

7. Click the **Apply on** box.
   The **Forests and Domains** pane appears.

8. (Optional) In the search box, type the forest or domain name.

9. Select the domain.

10. Click **Filter on selection**.

11. Make further customization as needed to the indicator for the selected domain.

12. Click **Save as draft**.
To discard the refined customization:

1. Click on tab for the customization.
2. Click **Remove this configuration** at the bottom of the pane.

See also

- [Create a Security Profile](#)
- [Delete a Security Profile](#)
- [Customize an Indicator](#)
- [Apply a Security Profile to a Workspace](#)
Delete a Security Profile

**Required User Role:** Administrator or organizational user with appropriate permissions.

To delete a security profile:

1. In Tenable.ad, click **Accounts > Security profiles management**.
   
The **Security profiles management** pane appears.

2. In the list of security profiles, hover over the security profile you want to delete and click on the icon at the end of the line.
   
   A message asks you to confirm the deletion.

3. Click Delete.
   
   A message confirms that Tenable.ad 3.x User and Administrator Guide deleted the profile.

See also

- [Create a Security Profile](#)
- [Customize an Indicator](#)
- [Refine Customization on an Indicator](#)
- [Apply a Security Profile to a Workspace](#)
User Roles

Tenable.ad uses Role-Based Access Control (RBAC) to secure access to data and functions within your organization. Roles determine the type of information that a user can access from their account depending on their role.

Users with appropriate permissions can assign permissions to other users based on their role to perform the following actions:

- Read contents and menus, system, and Indicator of Exposure configurations.
- Edit contents and menus, system and Indicator of Attack configurations.
- Create accounts, security profiles, and roles.

See also

- [Manage Roles](#)
- [Set Permissions for a Role](#)
- [Set Permissions on User Interface Entities (Example)](#)
Manage Roles

To create a new role:

1. In Tenable.ad 3.x User and Administrator Guide, go to Accounts > Roles management.
2. Click the Create a role button in the upper-right corner.
   The Create a role pane appears.
3. In the Name box, type the name for the role.
4. In the Description box, type some information about the role.
5. Click Add in the lower-right corner.
   A message appears confirms that Tenable.ad 3.x User and Administrator Guide created the role. The Edit a role pane appears for you to set permissions for the role.

Note: You cannot modify the Tenable.ad administrator role (called Global administrator). Click on the icon to display the Tenable.ad role settings.

To delete a role:

1. In Tenable.ad 3.x User and Administrator Guide, go to Accounts > Roles management.
2. In the list of roles, hover over the role you want to delete and click the icon on the right.
   A message asks you to confirm the deletion.
3. Click Delete.
   A message appears to confirm the deletion of the role.

See also

- Set Permissions for a Role
**Set Permissions for a Role**

**Required User Role:** Administrator or organizational user with appropriate permissions.

Tenable.ad 3.x User and Administrator Guide uses Role-Based Access Control (RBAC) to secure access to its data. A role determines what type of information users can access depending on their functional roles in the organization. When you create a new user in Tenable.ad, you assign that user a specific role with its associated permissions.

To set permissions for a role:

1. In Tenable.ad 3.x User and Administrator Guide, click **Accounts > Roles management**.
2. Hover over the role for which you want to set permissions and click the [icon on the right.](#)

   The **Edit a role** pane appears.

3. Under **Permissions Management**, select an entity type:
   - Data Entities
   - User Entities
   - System Configuration Entities
   - Interface Entities

4. In the list of entity names, select the entity to set permissions on.

5. Under the columns **Read, Edit, or Create**, click the toggle to Granted or Unauthorized.

6. You can either:
   - Click Apply to apply the permission and keep the **Edit a role** pane open for further modifications.
   - Click Apply and close to apply the permission and close the **Edit a role** pane.

   A message confirms that Tenable.ad 3.x User and Administrator Guide updated the role.

To set permissions in bulk for a role:
1. In Tenable.ad 3.x User and Administrator Guide, click **Accounts > Roles management**.

2. Hover over the role for which you want to set permissions and click the ⌬ icon on the right. The **Edit a role** pane appears.

3. Under **Permissions Management**, select an entity type.

4. Select the entities or section(s) of entities (for example Indicators of Exposure) to set permissions on.

5. At the bottom of the page, click the arrow on the drop-down box to display a list of permissions.

6. Select the permission(s) for the role.

7. Click **OK**.

A message confirms that Tenable.ad 3.x User and Administrator Guide set the permissions on the entities.

---

**Permission Types**

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read</td>
<td>Permission to view an object or a configuration.</td>
</tr>
<tr>
<td>Permission</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Edit</td>
<td>Permission to modify an object or a configuration. Requires the Read permission to apply modifications.</td>
</tr>
<tr>
<td>Create</td>
<td>Permission to create an object or a configuration. The <strong>Create</strong> permission requires the <strong>Read</strong> and <strong>Edit</strong> permissions to perform permitted actions on permitted resources.</td>
</tr>
</tbody>
</table>

## Entity Types

There are four types of entities in Tenable.ad 3.x User and Administrator Guide that require permissions to access which you can tailor for each user role in your organization:

<table>
<thead>
<tr>
<th>Entity Type</th>
<th>Contains</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Entities</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| This entity controls the permissions for setting up the monitored Active Directory and configuring the data analysis in Tenable.ad 3.x User and Administrator Guide. | • Indicators of Attack  
• Indicators of Exposure  
• Forests  
• Domains  
• Profiles  
• Users  
• Alerts by email  
• Alerts by Syslog  
• Roles | Read, Edit, Create |
| **User Entities** |                                                                                   |                 |
| This entity controls a user's ability to configure information that Tenable.ad 3.x User and Administrator Guide displays for data analysis and to modify personal information and  | • Preferences  
• Dashboards  
• Widgets  
• API key | Edit, Create |
| preferences. | • Maximum workload data  
  • Personal information |
| --- | --- |

### System Configuration Entities

This entity controls the access to the Tenable.ad 3.x User and Administrator Guide platform and services.

- Application services (SMTP, logs, authentication Tenable.ad, Indicators of Attack, PKI settings)
- Scores through public API
- Licences
- LDAP authentication
- SAML authentication
- Topology
- Accounts Lockout Policy
- Recrawl domains
- Change the max IOA workload quota

| Interface Entities |
| --- | --- | --- |
| This entity defines the permissions to access specific parts of the Tenable.ad 3.x User and Administrator Guide user interface and features. |
| Access paths to specific Tenable.ad 3.x User and Administrator Guide features. For more information, see [Set Permissions on User Interface Entities](#) (Example) |

### See also

- [User Accounts](#)
- [User Roles](#)
Set Permissions on User Interface Entities (Example)

Tenable.ad 3.x User and Administrator Guide applies permissions along the path used to access a certain user interface feature. The following example shows how to set permissions to allow the configuration of Syslog.

To reach Syslog parameters, users require permissions along the path **System > Configuration > SYSLOG** in Tenable.ad 3.x User and Administrator Guide:

- System configuration: **Management > System**
- Configuration parameters: **Management > System > Configuration**
- Syslog alerts: **Management > System > Configuration > Alerting engine > SYSLOG**

To set permissions for Syslog configuration:

1. In Tenable.ad 3.x User and Administrator Guide, click **Accounts > Roles management**.
2. Hover over the role for which you want to set permissions and click the 🔄 icon on the right.
   
   The **Edit a role** pane appears.
3. Under **Permissions Management**, select **Interface Entities**.
4. In the list of entities, do the following:
   
   - Select **Management > System** and click the Access toggle to **Granted**.
   - Select **Management > System > Configuration** and click the Access toggle to **Granted**.
   - Select **Management > System Configuration > Alerting engine > SYSLOG** and click the Access toggle to **Granted**.
5. Click **Apply**.

A message confirms that Tenable.ad 3.x User and Administrator Guide updated permissions on the entities.
6. Under **Permissions Management**, select **Data Entities**.

7. In the list of entity sections, select **Alerts by Syslog**.

8. Select the **Creation** permission.

   Tenable.ad 3.x User and Administrator Guide implicitly grants the Read and Edit permissions.

9. Click **Apply and Close**.

   A message confirms that Tenable.ad 3.x User and Administrator Guide updated permissions on the entities.
Forests

To add a forest:

1. In Tenable.ad 3.x User and Administrator Guide, click **System** > **Forest management**.
2. Click **Add a forest** on the right.
   
   The Add a forest pane appears.
3. In the **Name** box, type the forest name.
4. In the **Account** section, provide the following for the account that Tenable.ad 3.x User and Administrator Guide uses:
   
   - **Login**
   - **Password**
5. Click **Add**.

   A message confirms the addition a new forest.

To edit a forest:

1. In Tenable.ad 3.x User and Administrator Guide, click **System** > **Forest management**.
2. In the list of forests, hover over the forest you want to modify and click the ⌒ icon on the right.

   The **Edit a forest** pane appears.
3. Make the necessary modifications.
4. Click **Edit**.

   A message confirms that Tenable.ad 3.x User and Administrator Guide updated the forest.
Domains

Tenable.ad 3.x User and Administrator Guide monitors domains which group objects that share common settings in a logical manner for centralized management.

- Add a Domain
- Edit a Domain
- Delete a Domain
- Force Data Refresh on a Domain
- Honey Accounts
Add a Domain

To add a domain:


2. Click the Domain management tab.
   
   The Domain Management pane appears.

3. Click Add a domain in the upper-right corner.
   
   The Add a domain pane appears.

4. In the Main Information section, give the following information:
   
   • In the Name box, type the name of the domain.
   
   • In the Domain FQDN box, type the Fully Qualified Domain Name (FQDN) for the domain.
   
   • In the Forest drop-down box, select the forest to which the domain belongs.

5. In the Primary Domain Controller section, give the following information:
   
   • In the IP address or hostname box, type the primary domain controller's IP address or hostname.
   
   • In the LDAP port box, type the primary domain controller's LDAP port.
   
   • In the Global Catalog port box, type the primary domain controller's global catalog port.
   
   • In the SMB port box, type the primary domain controller's SMB port.

6. Click Add.
   
   A message appears to confirm that Tenable.ad 3.x User and Administrator Guide added the domain.

See also

• Edit a Domain

• Delete a Domain
- Force Data Refresh on a Domain
- Honey Accounts
Edit a Domain

To edit a domain:

2. Click the Domain management tab.
   The Domain Management pane appears.
3. Hover over the name of the domain you want to edit to display the icon on the right.
4. Click the icon.
   The Edit a domain pane appears.
5. Edit the information for the domain.
6. Click Edit.
   A message appears to confirm that Tenable.ad 3.x User and Administrator Guide updated the domain.

See also

- Add a Domain
- Delete a Domain
- Force Data Refresh on a Domain
- Honey Accounts
Delete a Domain

To delete a domain:


2. Click the Domain management tab.

   The Domain Management pane appears.

3. Hover over the name of the domain you want to delete to display the 🗑 icon.

4. Click the 🗑 icon.

   A message appears to ask you to confirm the deletion.

5. Click Delete.

   A message appears to confirm that Tenable.ad 3.x User and Administrator Guide deleted the domain.

See also

- Add a Domain
- Edit a Domain
- Force Data Refresh on a Domain
- Honey Accounts
Force Data Refresh on a Domain

To force data refresh on a domain:

2. Click the Domain management tab. The Domain Management pane appears.
3. Hover over the name of the domain on which you want to force data refresh to display the icon on the right.
4. Click the icon. A message appears with information about the data refresh action.
5. Click Confirm.

See also

- Add a Domain
- Edit a Domain
- Delete a Domain
- Honey Accounts
Honey Accounts

**Required User Role:** Administrator on the local machine

A Honey Account is a decoy account whose unique purpose is to detect an attacker trying to compromise the network through the Active Directory.

It is a prerequisite for Tenable.ad 3.x User and Administrator Guide's Indicator of Attack to detect Kerberoasting exploitation attempts which seek to gain access to service accounts by requesting and extracting service tickets and then cracking the service account's credentials offline. The Kerberoasting Indicator of Attack sends out alerts when the Honey Account receives login attempts or ticket requests.

You associate one Honey Account per domain. Honey Accounts are not related to security profiles.

To add a Honey Account:

1. In Tenable.ad 3.x User and Administrator Guide, click **Systems > Domain management**.
   The **Domain Management** pane appears.
2. Hover over the domain for which you want to add a Honey Account.
3. Under **Honey Account configuration status**, click +.
   The **Add a Honey Account** pane appears.
4. In the **Name** box, type a Distinguished Name (DN) for the user account to use as the Honey Account.
   
   **Tip:** You can type any string and Tenable.ad 3.x User and Administrator Guide searches for and displays matching user account names in the drop-down box if that user account already exists in the Active Directory.
5. In the **Deployment** section, Tenable.ad 3.x User and Administrator Guide generates a script with the appropriate settings for you to run to deploy the Honey Account. Click ⬅️ to copy this script.
6. Click **Add**.
A message appears to confirm that Tenable.ad 3.x User and Administrator Guide added the Honey Account. In the Domain Management pane, the selected domain's Honey Account configuration status appears orange (●) to indicate that you must run the Honey Account deployment script to activate it.

**Note:** If the Honey Account configuration status appears red (●), it indicates that Tenable.ad 3.x User and Administrator Guide did not find this user account in the Active Directory. You must create this user account and proceed to the next step.

7. In a Windows PowerShell on a machine with the Active Directory module, run the Honey Account deployment script that you copied.

In the Domain Management pane, the selected domain's Honey Account configuration status appears with an green status (●) to indicate that it is active.

**Note:** Tenable.ad 3.x User and Administrator Guide may take some time to process and activate the Honey Account.

To edit a Honey Account:

1. In Tenable.ad 3.x User and Administrator Guide, click **Systems > Domain management**.

The Domain Management pane appears.

2. Hover over the domain for which you want to add a Honey Account.

3. Under Honey Account configuration status, click the icon at the right.

The Edit a Honey Account pane appears.

4. In the Name box, modify the user account as necessary.

5. In the Deployment section, click to copy the Honey Account Deployment script.

6. Click Edit.

A message appears to confirm that Tenable.ad 3.x User and Administrator Guide updated the Honey Account. In the Domain Management pane, the selected domain's Honey Account configuration status appears orange (●) to indicate that you must run the Honey Account deployment script to activate it.
Note: If the **Honey Account configuration status** appears red (●), it indicates that Tenable.ad 3.x User and Administrator Guide did not find this user account in the Active Directory. You must create this user account and proceed to the next step.

7. In a Windows PowerShell on a machine with the Active Directory module, run the Honey Account deployment script that you copied.

    In the **Domain Management** pane, the selected domain's **Honey Account configuration status** appears with an green status (●) to indicate that it is configured.

    **Note:** Tenable.ad 3.x User and Administrator Guide may take some time to process and activate the Honey Account.

**To delete a Honey Account:**

1. In Tenable.ad 3.x User and Administrator Guide, click **Systems > Domain management.**

    The **Domain Management** pane appears.

2. Hover over the domain for which you want to add a Honey Account.

3. Under **Honey Account configuration status**, click the ● icon at the right.

    The **Edit a Honey Account** pane appears.

4. Click **Delete**.

    A message appears to confirm that Tenable.ad 3.x User and Administrator Guide deleted the Honey Account.

**See also**

- [Kerberoasting](#)
- [Add a Domain](#)
- [Edit a Domain](#)
- [Delete a Domain](#)
- [Force Data Refresh on a Domain](#)
**Attack Scenarios**

**Required User Role:** Organizational user with permissions to modify the Indicators of Attack configuration.

You define an attack scenario by selecting the types of attack for Tenable.ad to monitor on specific domains.

**Before you begin**

In order to modify the attack scenario, you must have a user role with the following permissions:

- In **Data Entities**, "Read" access for:
  - All Indicators of Attack
  - All domains

- In **Interface Entities**, access for:
  - Management > System > Configuration
  - Management > System > Configuration > Application Services > Indicators of Attack
  - Management > System > Configuration > Application Services > Indicators of Attack > Download installation file

For more information about role-based permissions, see [Set Permissions for a Role](#).

**To define an attack scenario:**

1. In Tenable.ad 3.x User and Administrator Guide, click on **Systems > Configuration > Indicators of Attack**.

   The **Definition of Attack Scenarios** pane opens.
2. Under **Attack Name**, select the attack to monitor.

3. Select the domain on which to monitor for the selected attack.

4. Optionally, you can do one of the following:
   - Click on **Select all** to monitor for all attacks on all domains.
   - Click on **n/n domains** or **n/n indicators** to filter for specific domains to monitor for specific attacks.

5. Click **Save**.

   A confirmation message informs you that Tenable.ad 3.x User and Administrator Guide clears the activity status of each attack after you save the configuration.

6. Click **Confirm**.

   A message confirms that Tenable.ad 3.x User and Administrator Guide updated the Indicator of Attack configuration.

7. Click **Download the installation file**.

8. For the new attack configuration to take effect, run the installation file:
a. Copy and paste the downloaded installation file to the DC in the monitored domain.

b. Open a PowerShell terminal with administrative rights.

c. In Tenable.ad, copy the commands under the Indicators of Attack section at the bottom of the window.

![Indicators of Attack](image)


d. In the PowerShell window, paste the commands to run the script.

See also

- [Workload Quota](#)
**Workload Quota**

**Required User Role:** Organizational user with permissions to edit the workload quota.

Each Indicator of Attack in Tenable.ad has an associated workload quota that takes into account the resources required to analyze data from an attack.

Tenable.ad 3.x User and Administrator Guide calculates the workload quota to limit the number of Indicators of Attack (IoAs) running simultaneously which has an impact on bandwidth and CPU usage for event generation on domain controllers.

After you modify the workload quota limit, do the following:

- **Increase:** Monitor statistics following the increase to ensure a comfortable margin.
- **Decrease:** Deactivate some IoAs to stay under this quota, which reduces security coverage against attacks.

To modify the workload quota limit:

1. In Tenable.ad 3.x User and Administrator Guide, click on **Systems > Configuration > Indicators of Attack**.

   The **Definition of Attack Scenarios** pane opens.

2. Under **Indicators of Attack**, in the **Quota maximum limit** box, type a value for the workload quota limit.
3. Click the checkmark next to the value you entered.

A message informs you of the modification's impacts on Tenable.ad.

**Note:** If you type a quota maximum limit that is smaller than what the current attack configuration requires, you must adjust the number of active Indicators of Attack or raise the limit.

4. Click **Confirm**.

A message confirms that Tenable.ad 3.x User and Administrator Guide updated the quota maximum limit.

5. Click **Save**.

A confirmation message informs you that Tenable.ad 3.x User and Administrator Guide clears the activity status of each attack after you save the configuration.

6. Click **Confirm**.

A message confirms that Tenable.ad 3.x User and Administrator Guide updated the Indicator of Attack configuration.

7. Click **Download the installation file**.
8. For the new attack configuration to take effect, run the installation file:
   a. Copy and paste the downloaded installation file to the DC in the monitored domain.
   b. Open a PowerShell terminal with administrative rights.
   c. In Tenable.ad, copy the commands under the Indicators of Attack section at the bottom of the window.

   ![Indicators of Attack](image)

   d. In the PowerShell window, paste the commands to run the script.

See also

- **Attack Scenarios**
- **Set Permissions for a Role**
Indicators of Attack and the Active Directory

**Required license:** Indicators of Attack

Tenable.ad 3.x User and Administrator Guide’s indicators of attack provide a reactive approach to detect an attack in real time. Tenable.ad leverages three sources of information to detect security incidents:

- Your Active Directory database
- The SYSVOL shared folder
- The Event Tracing for Windows (ETW) engine

Tenable.ad collects the insertion strings associated with the event IDs and processes them to determine whether or not the events represent an attack.

For information on how to install the Indicators of Attack module, see [Install Indicators of Attack](#).

### Indicators of Attack

Each indicator of attack (IoA) requires specific audit policies that the installation script automatically enables.

**Note:** You must run the IoA installation script again if the configuration for the attack detection changes.

- [Credential Dumping: LSASS Memory](#)
- [DCShadow](#)
- [DCSync](#)
- [Enumeration of Local Administrators](#)
- [GoldenTicket](#)
- [Kerberoasting](#)
- [Massive Computers Reconnaissance](#)
- [NTDS Extraction](#)
- Password Guessing
- Password Spraying
- PetitPotam
Credential Dumping: LSASS Memory

After a user logs on, attackers can attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). This indicator of attack requires the Sysmon extension 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>
</tbody>
</table>

Requires Sysmon extension

For information on how to install and configure Sysmon, see Install Microsoft Sysmon.

See also

- DCShadow
- DCSync
- Enumeration of Local Administrators
- GoldenTicket
- Kerberoasting
- Massive Computers Reconnaissance
- NTDS Extraction
- Password Guessing
- Password Spraying
- PetitPotam
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></td>
<td>- Category: Logon/Logoff</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Sub-category: Logon</td>
</tr>
<tr>
<td>4634</td>
<td></td>
<td>- Category: Logon/Logoff</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Sub-category: Logoff</td>
</tr>
<tr>
<td>4662</td>
<td></td>
<td>- Category: Directory Service (DS Access)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Sub-category: Directory Service Access</td>
</tr>
<tr>
<td></td>
<td><strong>Requires Sysmon extension</strong></td>
<td>No</td>
</tr>
</tbody>
</table>

See also

- [Credential Dumping: LSASS Memory](#)
- [DCSync](#)
- [Enumeration of Local Administrators](#)
- [GoldenTicket](#)
- [Kerberoasting](#)
- [Massive Computers Reconnaissance](#)
- [NTDS Extraction](#)
- [Password Guessing](#)
- [Password Spraying](#)
- [PetitPotam](#)
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>
</tbody>
</table>

Requires Sysmon extension

No

See also

- Credential Dumping: LSASS Memory
- DCSHadow
- Enumeration of Local Administrators
- GoldenTicket
- Kerberroasting
- Massive Computers Reconnaissance
- NTDS Extraction
- Password Guessing
- Password Spraying
- PetitPotam
Enumeration of Local Administrators

This Indicator of Attack (IoA) detects reconnaissance attacks that enumerate the members of the Local Administrator group on domain controllers. A common attack tool that attackers use is BloodHound, which this IoA can detect in BloodHound’s default configuration.

Tenable.ad supports two methods in this IoA:

- Targeted systems for Windows versions 2016 or later.
- Targeted systems for Windows versions 2012 R2 or earlier.

<table>
<thead>
<tr>
<th>Detection Type</th>
<th>Related to a Common Vulnerabilities and Exposures (CVE)</th>
<th>Available from Tenable.ad 3.x User and Administrator Guide version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic IOC</td>
<td>No</td>
<td>3.14</td>
</tr>
</tbody>
</table>

How the attack works

The attacker uses the SAMR RPC (Remote Procedure Call) interface to list the members of the local Administrators group (not a domain group) of some domain controllers.

How the IoA works

This IoA can detect this technique, which SharpHound3 (the crawler part of the BloodHound tool) uses when it is launched through the following configurations:

- Using the default configuration.
- Enabling all collection methods.
- Enabling only the LocalAdmin collection method.

In addition to BloodHound, this IoA can detect other attack tools that use the same technique.

You should not have false positives (especially for Windows versions 2016+) because the IoA detection relies on the Sharphound implementation, which differs from the Microsoft library. For this reason, the IoA does not consider as an attack such normal behaviors as the Microsoft Management Console (MMC) and command line tools that remotely list the members of the local Administrators group.
The IoA’s detection technique is different for systems running Windows versions earlier than 2012 R2, because Microsoft does not provide the required event for older systems. Tenable.ad provides another less robust algorithm and enables it by default for older systems. If required, you can disable this option in Tenable.ad.

**Note:** In most situations, this IoA triggers at the same time as the [Massive Computers Reconnaissance](#) IoA. This is expected because they do not cover exactly the same cases.

### Specific modifications to the environment

None. Tenable.ad adapts the audit policy to meet the needs of the required Windows event logs.

<table>
<thead>
<tr>
<th>Events auditing policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider Name</td>
</tr>
<tr>
<td><strong>Microsoft-Windows-Security-Auditing</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Microsoft-Windows-Security-Auditing</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Microsoft-Windows-Security-Auditing</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
### Handle Manipulation

<table>
<thead>
<tr>
<th>Other requirements</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Sysmon extension</td>
<td>No</td>
</tr>
<tr>
<td>Honey Account</td>
<td>No</td>
</tr>
</tbody>
</table>

**See also**

- [Credential Dumping: LSASS Memory](#)
- [DCShadow](#)
- [DCSync](#)
- [GoldenTicket](#)
- [Kerberoasting](#)
- [Massive Computers Reconnaissance](#)
- [NTDS Extraction](#)
- [Password Guessing](#)
- [Password Spraying](#)
- [PetitPotam](#)
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 ⊂ — Sub-category: Kerberos Authentication Service</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>4769</td>
<td>⊂ Category: Account Logon ⊂ — Sub-category: Kerberos Service Ticket Operations</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>4770</td>
<td>⊂ Category: Account Logon ⊂ — Sub-category: Kerberos Service Ticket Operations</td>
<td>Success</td>
</tr>
</tbody>
</table>

Requires Sysmon extension

No

See also

- Credential Dumping: LSASS Memory
- DCShadow
- DCSync
- Enumeration of Local Administrators
- Kerberoasting
- Massive Computers Reconnaissance
- NTDS Extraction
- Password Guessing
- Password Spraying
- PetitPotam
Kerberoasting

Kerberoasting is a type of attack that targets Active Directory service account credentials for offline password cracking.

This attack seeks to gain access to service accounts by requesting and extracting service tickets and then cracking the service account's credentials offline.

The Kerberoasting Indicator of Attack requires the activation of Tenable.ad 3.x User and Administrator Guide's Honey Account feature to send out an alert when there is a login attempt on the Honey Account or if this account receives a ticket request.

<table>
<thead>
<tr>
<th>Provider Name</th>
<th>Channel</th>
<th>Event ID</th>
<th>Audit Policies</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft-Windows-Security-Auditing</td>
<td>Security</td>
<td>4769</td>
<td>Category: Account Logon</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sub-category: Kerberos Service ticket operations</td>
<td></td>
</tr>
</tbody>
</table>

See also

- [Honey Accounts](#)
- [Credential Dumping: LSASS Memory](#)
- [DCShadow](#)
- [DCSync](#)
- [Enumeration of Local Administrators](#)
- [GoldenTicket](#)
- [Massive Computers Reconnaissance](#)
- [NTDS Extraction](#)
- [Password Guessing](#)
• Password Spraying
• PetitPotam
Massive Computers Reconnaissance

This Indicator of Attack (IoA) detects reconnaissance attacks that generate a massive number of authentication requests to Active Directory (AD) computers. A common attack tool that attackers use is BloodHound, which this IoA can detect in most scenarios.

This IoA supports the following two cases:

- An attacker using a domain-joined computer (for example a compromised machine after a phishing attack).
- An attacker using a computer outside of the domain (for example a rogue computer connected to the network).

<table>
<thead>
<tr>
<th>Detection Type</th>
<th>Related to a Common Vulnerabilities and Exposures (CVE)</th>
<th>Available from Tenable.ad 3.x User and Administrator Guide version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behavioral</td>
<td>No</td>
<td>3.14</td>
</tr>
</tbody>
</table>

How the attack works

This IoA focuses on massive authentication requests originating from specific attack tools. In particular, when an attacker uses SharpHound3 (the crawler part of BloodHound), this tool calls some Remote Procedure Call (RPC) functions on all domain machines with a DNS name that resolves and which it can reach via SMB on TCP/445. As a result, the attacker account must authenticate to these computers before it can proceed. This leads to a large number of authentication requests in a short period of time, which triggers this IoA.

In addition to BloodHound, this IoA can detect other attack tools that exhibit a similar behavior.

How the IoA works

Tenable.ad triggers this IoA when it finds a dedicated pattern in a combination of the following conditions: (Default behavior that you can modify through the IoA options.)

- **Volumetry**: During a 1-hour window, if there are authentication requests for more than 10% of the total number of computers in the AD (with a fixed limit of 300 computers).
• **Source:** The requests all come from the same machine IP and domain account.

• **Diversity:** The requests target different domain computers.

**Note:** Because various domain controllers can answer authentication requests, Tenable.ad aggregates the events from all domain controllers and does the calculation on the sum.

Tenable.ad 3.x User and Administrator Guide filters out the same attack during a 15-minute period to limit the number of security alerts. Examples:

• If an attacker launches the same attack multiple times during those 15 minutes, Tenable.ad 3.x User and Administrator Guide only raises one alert with this IoA.

• If an attack takes one hour to complete, Tenable.ad 3.x User and Administrator Guide triggers four alerts to remind you that the attack is still in progress.

**Note:** Tenable.ad 3.x User and Administrator Guide offers several configuration options for this IoA. You may need to adapt them depending on the size of each monitored domain (the number of domain-joined computers) to have the fastest possible detection without getting false-positives.

**Note:** In some situations, this IoA triggers at the same time as the Enumeration of Local Administrators IoA. This is expected because they do not cover exactly the same cases.

### Specific modifications to the environment

To analyze NTLM authentication requests, the IoA script **automatically** configures the policy settings on your domain controllers through the Tenable.ad 3.x User and Administrator Guide Group Policy Object (GPO), as follows:

<table>
<thead>
<tr>
<th>Location of the setting</th>
<th>Security policy setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Network security: Restrict NTLM: Audit NTLM authentication in this domain</td>
<td>Enable all</td>
</tr>
<tr>
<td></td>
<td>Network security: Restrict</td>
<td>Enable audit-</td>
</tr>
</tbody>
</table>
### Events Auditing Policy

<table>
<thead>
<tr>
<th>Provider Name</th>
<th>Channel</th>
<th>Event IDs</th>
<th>Audit Policies</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft-Windows-Security-Netlogon</td>
<td>Microsoft-Windows-NTLM/Operational</td>
<td>8004</td>
<td>Configuration through a dedicated log, enabled by security policy settings.</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| Microsoft-Windows-Security-Auditing               | Security                    | 4624      | - **Category:** Logon/Logoff  
- **Sub-category:** Logon                         | Success             |
| Microsoft-Windows-Security-Auditing               | Security                    | 4769      | - **Category:** Account Logon  
- **Sub-category:** Kerberos Service Ticket Operations | Success             |

**Note:** You can modify the options in bold.

### Other requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sysmon extension</td>
<td>No</td>
</tr>
<tr>
<td>Honey Account</td>
<td>No</td>
</tr>
</tbody>
</table>

### See also
• Credential Dumping: LSASS Memory
• DCSHadow
• DCSync
• Enumeration of Local Administrators
• GoldenTicket
• Kerberoasting
• NTDS Extraction
• Password Guessing
• Password Spraying
• PetitPotam
**NTDS Extraction**

NTDS exfiltration refers to the technique that attackers use to retrieve the NTDS.dit database that stores Active Directory secrets such as password hashes and Kerberos keys. Once retrieved, the attacker parses a copy of this file offline, providing an alternative to DCSync attacks for retrieval of the Active Directory's sensitive content.

This Indicator of Attack sends an alert when an event shows the creation of a shadow copy of the database file in an attempt to exfiltrate the NTDS.dit database.

<table>
<thead>
<tr>
<th>Detection Type</th>
<th>Related to a Common Vulnerabilities and Exposures (CVE)</th>
<th>Available from Tenable.ad 3.x User and Administrator Guide version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic IOC</td>
<td>No</td>
<td>3.15</td>
</tr>
</tbody>
</table>

**How the attack works**

Since the operating system constantly accesses the NTDS.dit file, an attacker cannot read this file while it's being modified. In order to retrieve the password hashes from the NTDS.dit file, an attacker must meet one of the following criteria:

- No shadow copy exists, so the attacker must create a new one to represent a backup or a snapshot of the "C:" volume to get access to the targeted NTDS.dit file.

- A shadow copy already exists, so the attacker has direct access to it.

Once the attacker creates a shadow copy, they only have to exfiltrate the NTDS.dit file from the shadow volume (e.g. `\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\windows\system32\ntds.dit`) to a location which they control.

A broad range of tools can carry out this type of attack, including legitimate administration Windows tools such as `vssadmin` or `esentut1`.

**How the IoA works**

The NTDS Extraction Indicator of Attack can detect a large variety of attack tools by correlating Windows events specific to each step of this attack. Two main events drive the detection algorithm: one specific to the creation of the shadow copy, and the other specific to the creation of a process on the
domain controller. This second step allows the detection of malicious exfiltration activity independently of the creation of a shadow copy.

As a consequence, the IoA can detect at an early stage any suspicious patterns linked to an exfiltration attack. Also, using others relevant Windows events, the IoA can provide a detailed description of an NTDS exfiltration attack.

**Specific modifications in the environment**

To have access to the full command line in the event Microsoft-Windows-Security-Auditing/4688, the IoA script automatically configures the policy settings on your domain controllers through the Tenable.ad Group Policy Object (GPO), as follows:

<table>
<thead>
<tr>
<th>Location of the setting</th>
<th>Security policy setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Configuration &gt; Administrative Templates &gt; System &gt; Audit Process Creation</td>
<td>Include command line in process creation events</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

**Events Auditing Policy**

<table>
<thead>
<tr>
<th>Provider Name</th>
<th>Channel</th>
<th>Event ID</th>
<th>Audit Policies</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VSSAudit</td>
<td>Security</td>
<td>8222</td>
<td>† Category: Object Access &lt;br&gt; † — Sub-category: Audit Application Generated</td>
<td>Success</td>
</tr>
<tr>
<td>Microsoft-Windows-Security-Auditing</td>
<td>Security</td>
<td>4688</td>
<td>† Category: Detailed Tracking &lt;br&gt; † — Sub-category: Audit Process Creation</td>
<td>Success</td>
</tr>
<tr>
<td>Microsoft-Windows-Security-Auditing</td>
<td>Security</td>
<td>5145</td>
<td>† Category: Object Access &lt;br&gt; † — Sub-category:</td>
<td>Success</td>
</tr>
<tr>
<td>Application</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-----</td>
<td>-----</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ESENT</td>
<td>325</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft-Windows-WMI-Activity</td>
<td>5857</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft-Windows-Security-Auditing</td>
<td>4624</td>
<td>Success</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Category: Logon/Logoff</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sub-category: Audit Logon</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft-Windows-Security-Auditing</td>
<td>4634</td>
<td>Success</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Category: Logon/Logoff</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sub-category: Audit Logoff</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft-Windows-Security-Auditing</td>
<td>4689</td>
<td>Success</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Category: Detailed Tracking</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sub-category: Audit Process Termination</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft-Windows-Security-Auditing</td>
<td>4674</td>
<td>Success / Failure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Category: Privilege Use</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sub-category: Audit Sensitive Privilege Use</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Other requirements**

<table>
<thead>
<tr>
<th>Sysmon extension</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Honey Account</td>
<td>No</td>
</tr>
</tbody>
</table>
See also

- [Credential Dumping: LSASS Memory](#)
- [DCShadow](#)
- [DCSync](#)
- [Enumeration of Local Administrators](#)
- [GoldenTicket](#)
- [Kerberoasting](#)
- [Massive Computers Reconnaissance](#)
- [Password Guessing](#)
- [Password Spraying](#)
- [PetitPotam](#)
- [SAM Name Impersonation](#)
Password Guessing

A brute-force password guessing attack consists of an attacker submitting many passwords or pass phrases and hoping to guess correctly eventually. The attacker systematically checks all possible passwords and pass phrases until it finds the correct one.

<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 — Sub-category: Logon</td>
<td>Success</td>
</tr>
<tr>
<td>4625</td>
<td>Category: Logon/Logoff — Sub-category: Logoff</td>
<td>Failure</td>
</tr>
<tr>
<td>4771</td>
<td>Category: Account Logon — Sub-category: Kerberos Authentication Serviced</td>
<td>Failure</td>
</tr>
<tr>
<td>4776</td>
<td>Category: Account Logon — Sub-category: Credential Validation</td>
<td>Success and Failure</td>
</tr>
</tbody>
</table>

Requires Sysmon extension

No

See also

- [Credential Dumping: LSASS Memory](#)
- [DCShadow](#)
- [DCSync](#)
- [Enumeration of Local Administrators](#)
- [GoldenTicket](#)
- [Kerberoasting](#)
- [Massive Computers Reconnaissance](#)
- [NTDS Extraction](#)
• Password Spraying
• PetitPotam
Password Spraying

Password spraying is an attack that attempts to access a large number of accounts with a single or a 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>
</table>
| 4624      | Category: Logon/Logoff  
L — Sub-category: Logon | Success         |
| 4625      | Category: Logon/Logoff  
L — Sub-category: Logoff | Failure         |
| 4771      | Category: Account Logon  
L — Sub-category: Kerberos Authentication Serviced | Failure         |
| 4776      | Category: Account Logon  
L — Sub-category: Credential Validation | Success and Failure |

Requires Sysmon extension

Value: No

See also

- [Credential Dumping: LSASS Memory](#)
- [DCShadow](#)
- [DCSync](#)
- [Enumeration of Local Administrators](#)
- [GoldenTicket](#)
- [Kerberoasting](#)
- [Massive Computers Reconnaissance](#)
- [NTDS Extraction](#)
- Password Guessing
- PetitPotam
PetitPotam

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

An attacker can use PetitPotam 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 PetitPotam, the IoA installation script enables automatically the Microsoft-Windows-EFS/Debug channel by adding the 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 before 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).

### Event IDs

<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&lt;br&gt;Sub-category: Logon</td>
<td>Success</td>
</tr>
<tr>
<td>4634</td>
<td>Category: Logon/Logoff&lt;br&gt;Sub-category: Logoff</td>
<td>Success</td>
</tr>
<tr>
<td>--</td>
<td>Requires Sysmon extension</td>
<td>No</td>
</tr>
</tbody>
</table>

### Event IDs

<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>

**See also**
• Credential Dumping: LSASS Memory
• DCShadow
• DCSync
• Enumeration of Local Administrators
• GoldenTicket
• Kerberoasting
• Massive Computers Reconnaissance
• NTDS Extraction
• Password Guessing
• Password Spraying
SAM Name Impersonation

The **SAM Name Impersonation** Indicator of Attack (IoA) detects an attacker who tries to exploit two vulnerabilities (CVEs) that Microsoft patched silently in November 2021: CVE-2021-42278 and CVE-2021-42287. CVE-2021-42287 is critical and can lead to an elevation of privileges on the domain from a standard account without any security skills.

This IoA detects both fully automated tools such as [noPac](https://npx.dev/npac) and [sam-the-admin](https://github.com/godlews/sam-the-admin), as well as manual attacks using [Rubeus](https://github.com/sabberteos/Rubeus) and [Impacket](https://impacket.github.io/) tools.

It provides protection until you can patch all domain controllers (DCs), which can take some time in large environments. Even after you patch all DCs, the IoA can trigger alerts if an attacker attempts a manual attack under certain conditions.

<table>
<thead>
<tr>
<th>Detection Type</th>
<th>Related to a Common Vulnerabilities and Exposures (CVE)</th>
<th>Available from Tenable.ad 3.x User and Administrator Guide version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic IOC</td>
<td>Yes (CVE-2021-42278 / CVE-2021-42287)</td>
<td>3.15</td>
</tr>
</tbody>
</table>

**How the attack works**

An attacker can exploit the CVE-2021-42287 vulnerability by sending a Kerberos service ticket request using the S4U2self mechanism and providing a spoofing account that does not currently exist in the Active Directory (AD). This prompts the domain controller to search whether or not a similar account name ending with $ exists. If an account with such a `sAMAccountName` attribute exists, the attacker can compromise this account instead of the one they provided initially.

So by controlling an account that looks like a DC (i.e. the `sAMAccountName` = the DC name, without the ending $), the attacker can pretend to be this DC and elevate privileges on the domain.

In most scenarios, the attacker follows this process using a standard user account:

1. Creates a new computer account, using the AD misconfiguration of the ms-DS-MachineAccountQuota attribute.
2. Removes the Service Principal Names (SPNs) added to this newly created computer account.
3. Renames this computer to the name of a DC, dropping the ending $.

4. Requests a Kerberos TGT for this computer account using the password from the account creation.

5. Renames this computer to its original name by adding back the ending $.

6. Requests a Kerberos service ticket using the S4U2self mechanism by presenting the previously obtained TGT, to target a service on a DC.

By default, in unhardened environments, any domain user can create up to 10 computer accounts in AD, which is the recommended quota for the ms-DS-MachineAccountQuota attribute. Even though this would harden the global AD configuration, it is not enough to protect the AD from this attack. In fact, this attack process can take place using a spoofing user account instead of a computer account.

Automated attack tools apply exactly the same process. But it is possible to adapt this attack to target other types of accounts that are not domain controllers, such as any workstation or server (i.e. tier-0 servers), the SSO account from AADConnect, Managed Service Accounts, etc.

How the IoA works

Based on the attack process described above, the SAM Name Impersonation IoA analyzes all Kerberos TGT requests to check if they are legitimate. Whenever there is a TGT request for an account, the IoA looks in its data to see if there is another account in the AD with the same name but with a $ at the end of its sAMAccountName attribute. If the IoA finds such an account, then it is an indication of an attack.

Example: The event log shows a TGT request for the account PRIV-SRV. If the IoA finds an account in the AD referenced by PRIV-SRV$ in the sAMAccountName attribute (a user, computer, MSA, etc.), it triggers an attack alert.

Note: In rare cases, a user and a computer may have the same sAMAccountName attribute. In this case, you can use the dedicated IoA option in Tenable.ad 3.x User and Administrator Guide to remove future alerts.

Specific modifications to the environment

None. Tenable.ad adapts the audit policy to meet the needs of the required Windows event logs.

Events Auditing Policy
<table>
<thead>
<tr>
<th>Provider Name</th>
<th>Channel</th>
<th>Event IDs</th>
<th>Audit Policies</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft-Windows-Security-Auditing</td>
<td>Security</td>
<td>4768</td>
<td>Category: Account Logon</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sub-category: Audit Kerberos Authentication Service</td>
<td></td>
</tr>
<tr>
<td>Microsoft-Windows-Security-Auditing</td>
<td>Security</td>
<td>4624</td>
<td>Category: Logon/Logoff</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sub-category: Audit Logon</td>
<td></td>
</tr>
</tbody>
</table>

Other requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sysmon extension</td>
<td>No</td>
</tr>
<tr>
<td>Honey Account</td>
<td>No</td>
</tr>
</tbody>
</table>

See also

- [Credential Dumping: LSASS Memory](#)
- [DCShadow](#)
- [DCSync](#)
- [Enumeration of Local Administrators](#)
- [GoldenTicket](#)
- [Kerberoasting](#)
- [Massive Computers Reconnaissance](#)
- [NTDS Extraction](#)
- [Password Guessing](#)
• **Password Spraying**

• **PetitPotam**
Alerts

License required: Depending on the type of alert you want to send, you may require licenses for Indicators of Attack or Indicators of Exposure.

Tenable.ad's alerting system helps you identify security regressions and/or attacks on your monitored Active Directory. It pushes analytics data about vulnerabilities and attacks in real-time through email or Syslog notification.

- SMTP Server Configuration
- Email Alerts
- Syslog Alerts
- Syslog and Email Alert Details
SMTP Server Configuration

Tenable.ad 3.x User and Administrator Guide requires Simple Mail Transfer Protocol (SMTP) configuration to send out alert notifications.

To configure the SMTP server:

1. In Tenable.ad 3.x User and Administrator Guide, click System > Configuration.
2. Under Application Services, select SMTP Server.
3. Provide the following information:
   - SMTP Server address
   - SMTP Server port
   - SMTP account
   - SMTP account password
4. To force a TLS-encrypted connection to the SMTP server, click the toggle SMTP TLS protocol to enabled.
5. To upgrade an unsecured connection to TLS, click the toggle SMTP StartTLS to enabled.
6. In the Email address of the sender box, provide an email address for Tenable.ad 3.x User and Administrator Guide to use when sending emails.
7. Click Save.

A message confirms that Tenable.ad 3.x User and Administrator Guide updated the SMTP parameters.
Email Alerts

Tenable.ad 3.x User and Administrator Guide sends out email alerts to notify you automatically if events reach a certain severity threshold and require remediation actions. The following is an example of an email alert:

This email is best viewed in an HTML-capable mail client.

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.

IoA details
To add an email alert:

1. In Tenable.ad 3.x User and Administrator Guide, click **System > Configuration > Email**.

2. Click the **Add an email alert** button on the right.

   The **Add an email alert** pane appears.

3. Under the **Main Information** section, provide the following:
   - In the **Email address** box, type the recipient’s email address to receive notifications.
   - In the **Description** box, type a description for the recipient address.

4. In the **Trigger the alert** drop-down list, select either:
   - **On each deviance**: Tenable.ad 3.x User and Administrator Guide sends out a notification on each deviant IoE detection.
   - **On each attack**: Tenable.ad 3.x User and Administrator Guide sends out a notification on each deviant IoA detection.

5. In the **Profiles** box, click to select the profile(s) to use for this email alert.

6. **Send alerts when deviances are detected during the initial analysis phase**: do one of the following:
   - Select the checkbox: Tenable.ad 3.x User and Administrator Guide sends out a large volume of email notifications when a system reboot triggers alerts.
   - Unselect the checkbox: Tenable.ad 3.x User and Administrator Guide does not send out email notifications when a system reboot triggers alerts.

7. **Severity threshold**: click the arrow of the drop-down box to select the threshold at which Tenable.ad 3.x User and Administrator Guide sends alerts.

8. Depending on the alert trigger you selected in Step 4:
   - **Indicators of Exposure**: If you set alerts to trigger on each deviance, click the arrow next to each severity level to expand the list of Indicators of Exposure and select the ones for which to send alerts.
○ **Indicators of Attack:** If you set alerts to trigger **on each attack**, click the arrow next to each severity level to expand the list of Indicators of Attack and select the ones for which to send alerts.

9. Click the **Domains** box to select the domains for which Tenable.ad 3.x User and Administrator Guide sends out alerts.

The Forests and Domains pane appears.

a. Select the forest or domain.

b. Click **Filter on selection**.

10. Click **Test the configuration**.

A message confirms that Tenable.ad 3.x User and Administrator Guide sent an email alert to the server.

11. Click **Add**.

A message confirms that Tenable.ad 3.x User and Administrator Guide created the email alert.

**To edit an email alert:**

1. In Tenable.ad 3.x User and Administrator Guide, click **System > Configuration > Email**.

2. In the list of email alerts, hover over the one you want to modify and click the 📋 icon at the end of the line.

   The **Edit an email alert** pane appears.

3. Make the necessary modifications as described in the procedure **To add an email alert**:

4. Click **Edit**.

   A message confirms that Tenable.ad 3.x User and Administrator Guide updated the alert.

**To delete an email alert:**

1. In Tenable.ad 3.x User and Administrator Guide, click **System > Configuration > Email**.

2. In the list of email alerts, hover over the one you want to delete and click the ⌼ icon at the end of the line.

   A message asks you to confirm the deletion.
3. Click **Delete**.

   A message confirms that Tenable.ad 3.x User and Administrator Guide deleted the alert.

**See also**

- [SMTP Server Configuration](#)
- [Syslog and Email Alert Details](#)
Syslog Alerts

Some organizations use SIEM (Security Information and Event Management) to gather logs on potential threats and security incidents. Tenable.ad 3.x User and Administrator Guide can push security information related to Active Directory to the SIEM Syslog servers to improve their alerting mechanisms.

To add a new Syslog alert:

1. In Tenable.ad 3.x User and Administrator Guide, click **System > Configuration > Syslog**.
2. Click the **Add a Syslog alert** button on the right.
   
   The **Add a Syslog alert** pane appears.
3. Under the **Main Information** section, provide the following:
   
   - In the **Collector IP address or hostname** box, type the server IP or hostname that receives notifications.
   - In the **Port** box, type the port number for the collector.
   - In the **Protocol** box, click the arrow to select either UDP or TCP.
     
     - If you choose TCP, select the **TLS** option checkbox if you want to enable TLS security protocol to encrypt the logs.
   - In the **Description** box, type a brief description for the collector.
4. In the **Trigger the alert** drop-down list, select one:
   
   - **On changes**: Tenable.ad 3.x User and Administrator Guide sends out a notification whenever an event that you specified occurs.
   - **On each deviance**: Tenable.ad 3.x User and Administrator Guide sends out a notification on each deviant IoE detection.
   - **On each attack**: Tenable.ad 3.x User and Administrator Guide sends out a notification on each deviant IoA detection.
5. In the Profiles box, click to select the profile(s) to use for this Syslog alert.

6. **Send alerts when deviances are detected during the initial analysis phase**: do one of the following:
   - Select the checkbox: Tenable.ad 3.x User and Administrator Guide sends out a large volume of email notifications when a system reboot triggers alerts.
   - Unselect the checkbox: Tenable.ad 3.x User and Administrator Guide does not send out email notifications when a system reboot triggers alerts.

7. **Severity threshold**: click the arrow of the drop-down box to select the threshold at which Tenable.ad 3.x User and Administrator Guide sends alerts.

8. Depending on the alert trigger you selected in Step 4:
   - **Event changes**: If you set alerts to trigger on changes, type an expression to trigger the event notification.
     
     You can either click on the \( \times \) icon to use the search wizard or type a query expression in the search box and click **Validate**.
   - **Indicators of Exposure**: If you set alerts to trigger on each deviance, click the arrow next to each severity level to expand the list of Indicators of Exposure and select the ones for which to send alerts.
   - **Indicators of Attack**: If you set alerts to trigger on each attack, click the arrow next to each severity level to expand the list of Indicators of Attack and select the ones for which to send alerts.

9. Click the Domains box to select the domains for which Tenable.ad 3.x User and Administrator Guide sends out alerts.

   The **Forests and Domains** pane appears.

   a. Select the forest or domain.
   
   b. Click **Filter on selection**.
10. Click **Test the configuration**.

   A message confirms that Tenable.ad 3.x User and Administrator Guide sent a Syslog alert to the server.

11. Click **Add**.

   A message confirms that Tenable.ad 3.x User and Administrator Guide created the Syslog alert.

**To edit a Syslog alert:**

1. In Tenable.ad 3.x User and Administrator Guide, click **System > Configuration > Syslog**.

2. In the list of Syslog alerts, hover over the one you want to modify and click the icon at the end of the line.

   The **Edit a Syslog alert** pane appears.

3. Make the necessary modifications as described in the procedure [To add a new Syslog alert](#).

4. Click **Edit**.

   A message confirms that Tenable.ad 3.x User and Administrator Guide updated the alert.

**To delete a Syslog alert:**

1. In Tenable.ad 3.x User and Administrator Guide, click **System > Configuration > Syslog**.

2. In the list of Syslog alerts, hover over the one you want to delete and click the icon at the end of the line.

   A message asks you to confirm the deletion.

3. Click **Delete**.

   A message confirms that Tenable.ad 3.x User and Administrator Guide deleted the alert.

**See also**

- [Syslog and Email Alert Details](#)
Syslog and Email Alert Details

The following is an example of an alert:

```
<116>Jun 7 05:37:03 customer.tenable.ad TenableAD [6]: "0" "1" "FOREST" "DOMAIN" "C-PASSWORD-DONT-EXPIRE" "medium"
"CN=s_infosec.scanner,OU=ADMangers,DC=domain,DC=local" "24933" "1" "L-DONT-EXPIRE-SET" "40667" "Cn = "s_infosec.scanner"

<113>Jun 8 05:37:03 customer.tenable.ad TenableAD [6]: "0" "1" "FOREST" "DOMAIN" "C-UNCONST-DELEG" "critical"
"CN=s_infosec.scanner,OU=ADMangers,DC=domain,DC=local" "38197" "1" "R-DELEG-PRIVUSERS-NOT-PROTECTED" "40670"
"Cn = "s_infosec.scanner", "PrivilegesPath" "CN=Backup Operators,CN=Builtin,DC=domain,DC=local"
```

Alert Structure

<table>
<thead>
<tr>
<th>Part</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>①</td>
<td>Time Stamp is the date of the detection. Example: &quot;Jun 7 05:37:03&quot;</td>
</tr>
<tr>
<td>②</td>
<td>Host Name is the name or IP address of your application. Example: &quot;customer.tenable.ad&quot;</td>
</tr>
<tr>
<td>③</td>
<td>Product Name is the name of the product on which the deviation was triggered. Example: &quot;TenableAD&quot;, &quot;AnotherTenableADProduct&quot;</td>
</tr>
<tr>
<td>④</td>
<td>PID is the product (Tenable.ad) ID. Example: [4] (invariable till now, as there is only one product)</td>
</tr>
<tr>
<td>⑤</td>
<td>Tenable Msg Type is the identifier of event sources. Example: &quot;0&quot; (= On each deviation), &quot;1&quot; (= On changes), &quot;2&quot; (= On each attack)</td>
</tr>
<tr>
<td>⑥</td>
<td>Tenable Alert ID is the unique ID of the alert. Example: &quot;0&quot;, &quot;132&quot;</td>
</tr>
<tr>
<td></td>
<td>Description</td>
</tr>
<tr>
<td>---</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>①</td>
<td>Forest Name is the forest name of the related event. Example: &quot;Corp Forest&quot;</td>
</tr>
<tr>
<td>②</td>
<td>Domain Name is the domain name related to the event. Example: &quot;tenable.corp&quot;, &quot;zwx.com&quot;</td>
</tr>
<tr>
<td>③</td>
<td>Tenable Codename is the codename of the Indicator-of-Exposure. Example: &quot;C-PASSWORD-DONT-EXPIRE&quot;, &quot;C-UNCONST-DELEG&quot;</td>
</tr>
<tr>
<td>④</td>
<td>Tenable Severity Level is the severity level of the related deviance. Example: &quot;critical&quot;, &quot;high&quot;, &quot;medium&quot;</td>
</tr>
<tr>
<td>⑤</td>
<td>AD Object is the Distinguished Name of the deviant object. Example: &quot;CN=s_infoscan,OU=ADMangers,DC=domain,DC=local&quot;</td>
</tr>
<tr>
<td>⑥</td>
<td>Tenable Deviance ID is the ID of the deviance. Example: &quot;24980&quot;, &quot;132&quot;</td>
</tr>
<tr>
<td>⑦</td>
<td>Tenable Profile ID is the ID of the profile on which the deviance was triggered. Example: &quot;1&quot; (Tenable), &quot;2&quot; (i.e. soc_team)</td>
</tr>
<tr>
<td>⑧</td>
<td>AD Reason Codename is the codename of the deviance reason. Example: &quot;R-DONT-EXPIRE-SET&quot;, &quot;R-UNCONST-DELEG&quot;</td>
</tr>
<tr>
<td>⑨</td>
<td>Tenable Event ID is the ID of the event triggered by the deviance. Example: &quot;40667&quot;, &quot;28&quot;</td>
</tr>
<tr>
<td>⑩</td>
<td>Tenable Insertion Strings Name is the attribute name which was triggered on the deviant object. Example: &quot;Cn&quot;, &quot;useraccountcontrol&quot;, &quot;member&quot;, &quot;pwdlastset&quot;</td>
</tr>
<tr>
<td>⑪</td>
<td>Tenable Insertion Strings Value is the value of the attribute which was triggered on the deviant object. Example: &quot;s_infoscan&quot;, &quot;CN=Backup Operators,CN=Built,DC=domain,DC=local&quot;</td>
</tr>
</tbody>
</table>
**NOT FORCED TO CHANGE PASSWORD**

The `i_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 `i_infosec.scanner` account is privileged (`CN=Backup Operators,CN=BuiltIn,CN=`, 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 `i_infosec.scanner` and 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 `i_infosec.scanner` account hasn't been changed since 2020-10-28T19:47:16Z. The value derived from the `pwdLastSet` attribute is 730 days. The `i_infosec.scanner` account is considered as deviant. An account which doesn't regularly change its password is exposed to a higher risk of compromise.
<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>
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 interface showing About and License sections](image)

2. Click **Update the license file**.

3. Browse to the location of your license file and click **Open**.