<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Welcome to Tenable.ad</td>
<td>7</td>
</tr>
<tr>
<td>Get Started with Tenable.ad</td>
<td>8</td>
</tr>
<tr>
<td>Connection to Tenable.ad</td>
<td>10</td>
</tr>
<tr>
<td>User Preferences</td>
<td>12</td>
</tr>
<tr>
<td>Navigate Tenable.ad</td>
<td>14</td>
</tr>
<tr>
<td>Notifications</td>
<td>18</td>
</tr>
<tr>
<td>Dashboards</td>
<td>21</td>
</tr>
<tr>
<td>Widgets</td>
<td>23</td>
</tr>
<tr>
<td>Topology</td>
<td>28</td>
</tr>
<tr>
<td>Trust Relationships</td>
<td>30</td>
</tr>
<tr>
<td>Dangerous Trusts</td>
<td>33</td>
</tr>
<tr>
<td>Trail Flow</td>
<td>35</td>
</tr>
<tr>
<td>Trail Flow Table</td>
<td>37</td>
</tr>
<tr>
<td>Search the Trail Flow Using the Wizard</td>
<td>39</td>
</tr>
<tr>
<td>Search the Trail Flow Manually</td>
<td>41</td>
</tr>
<tr>
<td>Search History</td>
<td>44</td>
</tr>
<tr>
<td>Search Bookmarks</td>
<td>46</td>
</tr>
<tr>
<td>Display Deviant Events</td>
<td>48</td>
</tr>
<tr>
<td>Event Details</td>
<td>50</td>
</tr>
<tr>
<td>Attribute Changes</td>
<td>54</td>
</tr>
<tr>
<td>Trail Flow Use Cases</td>
<td>59</td>
</tr>
<tr>
<td>Attack Path</td>
<td>65</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Edit a User</td>
<td>222</td>
</tr>
<tr>
<td>Deactivate a User</td>
<td>223</td>
</tr>
<tr>
<td>Delete a User</td>
<td>224</td>
</tr>
<tr>
<td>Security Profiles</td>
<td>225</td>
</tr>
<tr>
<td>Create a Security Profile</td>
<td>226</td>
</tr>
<tr>
<td>Apply a Security Profile to a Workspace</td>
<td>228</td>
</tr>
<tr>
<td>Customize an Indicator</td>
<td>229</td>
</tr>
<tr>
<td>Refine Customization on an Indicator</td>
<td>232</td>
</tr>
<tr>
<td>Delete a Security Profile</td>
<td>234</td>
</tr>
<tr>
<td>User Roles</td>
<td>235</td>
</tr>
<tr>
<td>Manage Roles</td>
<td>236</td>
</tr>
<tr>
<td>Set Permissions for a Role</td>
<td>237</td>
</tr>
<tr>
<td>Set Permissions on User Interface Entities (Example)</td>
<td>241</td>
</tr>
<tr>
<td>Forests</td>
<td>244</td>
</tr>
<tr>
<td>Domains</td>
<td>245</td>
</tr>
<tr>
<td>Add a Domain</td>
<td>246</td>
</tr>
<tr>
<td>Edit a Domain</td>
<td>248</td>
</tr>
<tr>
<td>Delete a Domain</td>
<td>249</td>
</tr>
<tr>
<td>Force Data Refresh on a Domain</td>
<td>250</td>
</tr>
<tr>
<td>Honey Accounts</td>
<td>251</td>
</tr>
<tr>
<td>Attack Scenarios</td>
<td>254</td>
</tr>
<tr>
<td>Workload Quota</td>
<td>257</td>
</tr>
<tr>
<td>Indicators of Attack and the Active Directory</td>
<td>260</td>
</tr>
<tr>
<td>Credential Dumping: LSASS Memory</td>
<td>262</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>DCShadow</td>
<td>264</td>
</tr>
<tr>
<td>DCSync</td>
<td>265</td>
</tr>
<tr>
<td>Domain Backup Key Extraction</td>
<td>266</td>
</tr>
<tr>
<td>Enumeration of Local Administrators</td>
<td>270</td>
</tr>
<tr>
<td>GoldenTicket</td>
<td>273</td>
</tr>
<tr>
<td>Kerberoasting</td>
<td>275</td>
</tr>
<tr>
<td>Massive Computers Reconnaissance</td>
<td>277</td>
</tr>
<tr>
<td>NTDS Extraction</td>
<td>281</td>
</tr>
<tr>
<td>Password Guessing</td>
<td>285</td>
</tr>
<tr>
<td>Password Spraying</td>
<td>287</td>
</tr>
<tr>
<td>PetitPotam</td>
<td>289</td>
</tr>
<tr>
<td>SAM Name Impersonation</td>
<td>291</td>
</tr>
<tr>
<td>Alerts</td>
<td>295</td>
</tr>
<tr>
<td>SMTP Server Configuration</td>
<td>296</td>
</tr>
<tr>
<td>Email Alerts</td>
<td>297</td>
</tr>
<tr>
<td>Syslog Alerts</td>
<td>301</td>
</tr>
<tr>
<td>Syslog and Email Alert Details</td>
<td>304</td>
</tr>
<tr>
<td>Update Your License</td>
<td>309</td>
</tr>
</tbody>
</table>
Welcome to Tenable.ad

Last updated: 4/6/2022

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

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
- [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 misconfigurations 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 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 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 page opens.

**Caution:** If you repeatedly fail to log in, Tenable.ad locks your account. Contact your administrator.

To sign out of Tenable.ad:

1. In Tenable.ad 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

- **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 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.
c. Click **Save**.

A message confirms that Tenable.ad 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 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 ✂ 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 to deactivate the current token.

For more details, see Use Public API.
Navigate Tenable.ad

After you log in to Tenable.ad, 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 way security in an Active Directory</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</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. 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 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 can detect attacks in real-time.</td>
</tr>
<tr>
<td>9.</td>
<td><strong>Topology</strong> 🌐</td>
<td>The Topology page gives an interactive graph visualization of your Active Directory. It displays the forests, domains and trust relationships that</td>
</tr>
</tbody>
</table>
| 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 | 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 Administrator Guide](#).

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

| 12. | User Preferences | This page allows you to configure your language, profile, and password.

| 13. | Log out | Click to log out of Tenable.ad.

| 14. | Widgets | Widgets are customizable datasets |
| that a dashboard displays. They can contain bar charts, line charts, and counters. |
Notifications

At the top right of the Tenable.ad 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 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, 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
2. Click the **Deviances** tab.

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

![Diagram of deviances pane](image)

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, 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 created the dashboard. The new dashboard has a tab under **Dashboards**.

To rename a dashboard:

1. In Tenable.ad, 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 updated the dashboard.

To delete a dashboard:

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

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**.
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 added the widget.

**To modify a widget:**

1. In Tenable.ad, 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 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, 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 deleted the widget from the dashboard.
Topology

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

![Topology Graph](image)

To open the Topology page:

- In Tenable.ad, 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 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.

**See also**

• [Trust Relationships](#)

• [Dangerous Trusts](#)
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 displays the trust relationships displaying specific attributes between two entities.

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

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

For more information, see [Dangerous Trusts](#).

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><strong>Non-transitive</strong></td>
<td>By default, intra-forest trusts are transitive trusts. Tenable.ad uses this flag to convert them into non-transitive trusts. On the other hand, inter-</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Forest trusts</td>
<td>Forest trusts are non-transitive by default, hence the presence of the forest transitive flag. Tenable.ad displays this value 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>Within forest</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 QuarantinedWithinForest.</td>
</tr>
<tr>
<td>Up level only</td>
<td>Indicates that only clients running Windows 2000 operating systems and later can use this trust.</td>
</tr>
<tr>
<td>Treat as external</td>
<td>(Only when FOREST_TRANSITIVE applies) Indicates an external type of trust. Tenable.ad 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>Quarantined</td>
<td>Indicates that Tenable.ad enabled the filtering of the SIDs whose RID is greater than or equal to 1000 for the trust. By default, Tenable.ad 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>Cross-organization authentication</td>
<td>Indicates that Tenable.ad enabled selective authentication and can use it across domain or forest trusts.</td>
</tr>
<tr>
<td>Selective authentication</td>
<td>See Cross-organization authentication.</td>
</tr>
<tr>
<td>Cross organization without TGT delegation</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>RC4 encryption:</td>
<td>Indicates that the trust supports RC4-encryption keys for Kerberos exchanges. This flag is present only if the trustType applies to TRUST_</td>
</tr>
<tr>
<td>TYPE/MIT.</td>
<td>Indicators</td>
</tr>
<tr>
<td>-----------</td>
<td>------------</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 apply and the QUARANTINED_DOMAIN flag is not on, 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 act to implement bastion forests.</td>
</tr>
<tr>
<td><strong>No attribute</strong></td>
<td>Indicates that the external trust has no specific attribute.</td>
</tr>
</tbody>
</table>
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** pane 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.

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

To export deviant objects:
1. On the topology graph, click on the curved arrows.
   
   The **Deviant objects related to trusts** pane opens.

2. Click **Export all**.

   The **Export deviant objects** pane opens.

3. In the **Export format** box, click the drop-down arrow to select a format.

4. Click **Export all**.

   Tenable.ad downloads a file in the selected format to your computer.

5. Click **X** to close the pane.
Trail Flow

Tenable.ad's Trail Flow displays the real-time monitoring and analysis of events affecting your AD infrastructures. It allows you to identify critical vulnerabilities and their recommended courses of remediation.

Using the Trail Flow page, you can go back in time and load previous events or search for specific events. You can also use its search box at the top of the page to search for threats and detect malicious patterns.

To access the Trail Flow:

- In Tenable.ad, click Trail Flow in the navigation bar on the left.

The Trail Flow page opens with a list of events. For more information, see Trail Flow Table.

To select a timeframe:

1. At the top of the Trail Flow page, click on the calendar box.
2. Select a start date and an end date.
3. Click **Search**.
   Tenable.ad updates the Trail Flow table with the selected timeframe.

To select a domain:

1. At the top of the **Trail Flow** page, click **n/n domain >**.
   The **Forest and Domains** pane opens.
2. Select the forests and domains.
3. Click **Filter on selection**.
   Tenable.ad updates the Trail Flow table with information for the selected forest and domain.

To view an event:

- In the Trail Flow table, click on a line that contains the event you want to explore.

  The Event Details pane appears. For more information, see **Event Details**.

To pause and restart the Trail Flow:

- Do one of the following:
  - Click on the **่อ** icon to pause the Trail Flow.
    Pausing the Trail Flow stops the automatic vertical scrolling of the most recent events while the analysis continues to run in the background and allows you to run a search on events.
  - Click on the **ถ่าย** icon to restart the Trail Flow.

To load next or previous events:

- In the Trail Flow page, do one of the following:
  - Click Load next events
  - Click Load previous events
**Trail Flow Table**

Tenable.ad lists the events in your Active Directory in the Trail Flow table continuously as they occur. It includes the following information:

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Indicates the origin of any security-related change in your AD infrastructures. There are two possible sources:  - Lightweight Directory Access Protocol (LDAP) used to communicate with your AD infrastructure.  - Server Message Block (SMB) protocol used to share files, printers, etc.</td>
</tr>
</tbody>
</table>

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

**Note:** Active Directory (AD) allows administrators to create group policies that control settings deployed on user and machine accounts. The Group Policy Object (GPO) stores these control settings. The Sysvol folder stores GPO files on the domain controller. It is important to monitor the contents of GPOs for the security of your AD because each domain member can apply or execute them with a high level of privileges.

<table>
<thead>
<tr>
<th>Type</th>
<th>Shows the characteristic elements of an event such as:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• ACL changed</td>
</tr>
<tr>
<td></td>
<td>• SPN changed</td>
</tr>
<tr>
<td></td>
<td>• Member removed</td>
</tr>
<tr>
<td></td>
<td>• New member</td>
</tr>
<tr>
<td></td>
<td>• New trust</td>
</tr>
<tr>
<td></td>
<td>• Unknown file type added</td>
</tr>
<tr>
<td></td>
<td>• New object</td>
</tr>
<tr>
<td></td>
<td>• Object removed</td>
</tr>
</tbody>
</table>
- Password changed
- UAC changed
- New GPO linked
- GPO link removed
- Owner change
- File renamed
- SPN created
- Failed authentication reset
- Failed authentication

<table>
<thead>
<tr>
<th><strong>Object</strong></th>
<th>Indicates the class or file extension associated with an AD object. You can search for a directory object (user, computer, etc.) or a file with a specific file name extension (ini, XML, csv).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Path</strong></td>
<td>Indicates the full path to an AD object to identify the unique location of this object in the AD.</td>
</tr>
<tr>
<td><strong>Directory</strong></td>
<td>Indicates the directory from which the change in your AD infrastructure came.</td>
</tr>
<tr>
<td><strong>Date</strong></td>
<td>Indicates the time of the event.</td>
</tr>
</tbody>
</table>
Search the Trail Flow Using the Wizard

The search wizard allows you to create query expressions.

- When you use frequent expressions in the search box, you can add them to a list of bookmarks for later use.
- When you enter an expression in the search box, Tenable.ad saves this expression in its History pane for you to reuse.

To search using the wizard:

1. In Tenable.ad, click Trail Flow to open the Trail Flow page.
2. Click on the icon.

The Edit Query Expression pane opens.
3. To define the query expression in the panel, click on the **AND** or the **OR** operator button to apply to the first condition.

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

5. Do any of the following:
   - To add an attribute, click **Add a new rule**.
   - To add another condition, click **Add a new condition** + **AND** or **OR** operator. Select an attribute from the drop-down menu and enter its value.
   - To restrict the search to deviant objects, click the **Deviant only** toggle to allow. Select the **+AND** or **+OR** operator to add the condition to the query.
   - To delete a condition or rule, click the icon.

6. Click **Validate** to run the search or **Reset** to modify your query expressions.
Search the Trail Flow Manually

To filter events that match specific character strings or patterns, you can type an expression in the search box to refine results using the Boolean operators *, AND, and OR. You can encapsulate OR statements with parentheses to modify search priority. The search looks for any specific value in an Active Directory attribute.

To search the Trail Flow manually:

1. In Tenable.ad, click Trail Flow to open the Trail Flow page.
2. In the Search box, enter a query expression.

Example:

The following example searches for:
- Deactivated user accounts that can endanger monitored AD infrastructures.
- Suspicious activities and anomalous account use.

Grammar and Syntax

A Trail Flow query expression uses the following grammar and syntax:

- **Grammar**: `EXPRESSION [OPERATOR EXPRESSION]` *
- **Syntax**: `_KEY_ _SELECTOR_ _VALUE_

where:

- `_KEY_` refers to the AD object attribute to search (such as CN, userAccountControl, members, etc.)
- `_SELECTOR_` refers to the operator: : , >, <, >=, <=.
VALUE refers to value to search for.

You can use more keys to look for specific content:

- date looks for a specific date.
- isDeviant looks for events that created a deviance.

You can combine multiple Trail Flow query expressions using the **AND** and **OR** operators.

Examples:

- Look for all objects containing the string alice into the common name attribute: cn:"alice"

- Look for all objects containing the string alice in the common name attribute and which created a specific deviance: cn:"alice" and isDeviant:"true"

- Look for every event that occurred on 15 March 2022: date="2022-03-15 00:00:00"

- Look for a GPO named Default Domain Policy: objectClass:"groupPolicyContainer" and displayName:"Default Domain Policy"

- Look for all deactivated accounts with a SID containing S-1-5-21: userAccountControl:"DISABLE" and objectSid:"S-1-5-21"

- Look for all script.ini files in Sysvol: globalpath:"sysvol" and types:"SCRIPTSini"
Search History

When you enter an expression in the search box, Tenable.ad saves this expression in its History pane for you to reuse.

To use a query expression in the history:

1. In Tenable.ad, click **Trail Flow** to open the Trail Flow page.
2. Click inside the Search box.
   - The **History** and **Bookmarks** tab appear under the Search box.
3. Click the **History** tab.
   - The list of query expressions appears.
4. Click to select a query expression to use.
   - Tenable.ad loads the query expression and runs the search.

To manage your query expression history:
1. In Tenable.ad, click **Trail Flow** to open the Trail Flow page.

2. Click inside the Search box.

   The **History** and **Bookmarks** tab appear under the Search box.

3. Click the **History** tab.

   The list of query expressions appears.

4. Click **Manage your history**.

   The **History** pane opens.

5. Do any of the following:

   - **Search for a query expression:**
     a. Type a query expression in the Search box.
     b. Click the calendar box to select a start date and an end date.
     c. Click **Search**.

   - **To delete a query expression from the history:**
     - Click the **icon**.

   - **To clear all query expressions from the history:**
     a. Click **Clear selection**.

       A message asks you to confirm the deletions.

     b. Click **Confirm**.
**Search Bookmarks**

When you use frequent query expressions, you can add them to a list of customized bookmarks to use again.

To bookmark a query expression:

1. In Tenable.ad, click **Trail Flow** to open the Trail Flow page.

2. Click the 🌟 icon next to the Search box.
   
   The **Edit Query Expression** pane opens.

3. Type a query expression in the Search box.

4. Click the ⭐ icon at the right of the Search box.
   
   The **Add to Your Bookmarks** box appears.

5. In the **Choose a folder** box, click the drop-down arrow to select a folder from the list.

6. (Optional) Click the **Create a new folder** toggle to **Yes**. In the **Name of the folder** box, type a name for the bookmarks folder.

7. In the **Name of the bookmark** box, type a name for the bookmark.

8. Click **Add**.
   
   A message confirms that Tenable.ad added the bookmark to the list.

To use a bookmarked query expression:

1. In Tenable.ad, click **Trail Flow** to open the Trail Flow page.

2. Click inside the Search box.
   
   The **History** and **Bookmarks** tab appear under the Search box.

3. Click the **Bookmarks** tab.
   
   The list of bookmarks appears.

4. Click the bookmark to select it.
   
   Tenable.ad loads the query expression and runs the search.
To manage your bookmarks:

1. In Tenable.ad, click **Trail Flow** to open the Trail Flow page.
2. Click inside the Search box.
   - The **History** and **Bookmarks** tab appear under the Search box.
3. Click the **Bookmarks** tab.
   - The list of bookmarks appears.
4. Click **Manage your bookmarks**.
   - The **Bookmarks** pane opens.
5. Do any of the following:
   - **Search for a bookmark**:
     a. Type the bookmark name in the Search box.
     b. Select a folder from the drop-down list.
   - **Edit the name of a bookmark or a bookmark folder**:
     a. Click the icon for the bookmark or bookmark folder.
     b. In the **Name of the bookmark** or **Name of the folder** box, type a new name for the bookmark or the bookmark folder.
     c. Click **Edit**.
     - A message confirms that Tenable.ad updated the bookmark or bookmark folder name.
   - **Delete a bookmark of bookmark folder**:
     - Click the icon for the bookmark or bookmark folder.
Display Deviant Events

You can zero in directly on deviant events in the Trail Flow table.

To display only deviant events:

1. In Tenable.ad, click **Trail Flow** to open the Trail Flow page.
2. Click the 🦜 icon next to the Search box.
   
   The **Edit Query Expression** pane opens.
3. Click the **Deviant only** toggle to Allow.
4. Click **Validate**.

Tenable.ad updates the Trail Flow table with a list of events with a red diamond next to the source.
where:

- The Trail Flow detected a deviance in the Tenable.ad security profile.
- The Trail Flow detected a deviance in other security profiles.
- Shows that changes resolved the deviance.
Event Details

The Trail Flow in Tenable.ad provides detailed information on each event affecting your Active Directory (AD). Details on a specific event allow you to review technical information and take remedial actions that the Indicator of Exposure (IoE)’s severity level requires.

To view event details:

1. In Tenable.ad, click **Trail Flow** to open the Trail Flow page.

2. Click to select an entry in the Trail Flow table.
   
   The Event details pane opens.

IoE, Event, and Deviant Object

- An **Indicator of Exposure** (IoE) describes a threat that affects the AD. Tenable.ad’s IoEs assesses security levels after receiving an event in real time. IoEs can include several technical vulnerabilities. IoEs provide information on detected vulnerabilities, associated deviant objects, and recommendations for remedial actions.

- An **event** indicates a change related to security that can appear in an AD. It can be a password change, a user creation, a new or modified GPO, or 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 – either on its own or associated with another deviant object – that allows the IoE’s attack vector to work.
### Attributes Table

The Attributes table includes the following columns:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attributes</td>
<td>Indicates the attributes of the AD object associated with the event that you 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 that the event occurred.</td>
</tr>
<tr>
<td>Current value</td>
<td>Indicates the value of the attribute in the AD at the moment when you are viewing it.</td>
</tr>
</tbody>
</table>
Tip: To display the value of the attribute before the event occurred, hover the blue dot on the left (if any).

To search for an attribute:

- In the **Event details** pane, type a string in the Search box.

  Tenable.ad narrows the list to attributes matching the search string.

For more information, see [Attribute Changes](#).

### Deviances

If an event in the Trail Flow contains deviances, the Event Details pane also displays them to allow you to drill down to the source of the problem.

To display deviances:

1. In Tenable.ad, click **Trail Flow** to open the Trail Flow page.
2. Click to select an entry in the Trail Flow table.

   The **Event details** pane opens.
3. Select the **Deviances** tab.

   Tenable.ad displays the list of deviances and the IoEs that triggered them.

![Tenable.ad Deviances Example](image)

To drill-down to IoE details:
1. In the **Deviances** tab, click on the IoE tile below the reason for the deviance.

   The **Indicator details** pane opens with a list of deviant objects and the following information:
   
   - Name of the IoE
   - The severity of the IoE (Critical, High, Medium, Low)
   - The IoE status
   - The timestamp of the latest detection

2. Click on any of the following tabs:
   
   - **Information** – Includes internal and external resources on the IoE.
   - **Vulnerability details** – Provides explanations for the weakness detected in your AD.
   - **Deviant objects** – Includes technical details and a search box to filter for objects.
   - **Recommendations** – Includes tips on how to solve the issue.
Attribute Changes

When the value of an attribute changes, the Trail Flow shows a blue dot before the Attribute column.

To display the attribute change:

1. In Tenable.ad, click Trail Flow in the navigation bar on the left.

   The Trail Flow page opens with a list of events

2. Hover the blue dot in front of the event line to display the changes.

   The color of the Value at event label depends on the changes applied to the attribute:
   
   - Green – Addition
   - Red – Deletion
The `ntsecuritydescriptor` Attribute

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

To display details of an object security descriptor:

1. In Tenable.ad, click **Trail Flow** to open the Trail Flow page.
2. Click to select an entry in the Trail Flow table.

   The **Event details** pane opens.
3. Hover over the ntsecuritydescriptor attribute entry (Value at event or Current value column)**.

4. Click on **See SDDL Description**.

   The **SDDL Description** pane opens.

5. Click on the arrows on the left of the SDDL (1), DACL (2), and Descriptor (3) to expand the
6. Browse to an Access Control Entry (ACE) (4) highlighted in color to display the object's access rights. The color codes indicate:

- **Red** – Users have dangerous rights assigned to them and they must not have access rights to the object.

- **Orange** – Privileged users have dangerous rights assigned to them but they generally have this type of right (for example: Domain Admins).
- **Green** – There are no dangerous rights.

7. To copy the SDDL description, click **Copy to clipboard**.
Trail Flow Use Cases

To understand the Trail Flow behavior, two examples illustrate how an operation that you perform in your Active Directory (AD) interface reflects in the Trail Flow page.

Each example compares data from the administrator's side (in the AD interface) with the data from the end user's side (in Tenable.ad). Whether you use an application, API, or service to carry out an operation on your AD, the result on the Trail Flow is the same.

**Note:** These examples are not exhaustive and cannot cover every possible situation.

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

- On the administrator side, you enter various information on the new user account.
• On the end-user side, Tenable.ad updates the **Trail Flow** page. See the **Type** column indicating *New object*.

![Trail Flow page](image)

• The **Event details** page also reflects this change. The blue dots on the left of the attribute names indicate that an update 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 side, you enter various information to reset a user's password.
• On the end-user side, Tenable.ad updates the **Trail Flow** page. See the **Type** column indicating "Password changed."

![Screenshot of the Trail Flow page showing a search bar and a list of events with a blue dot on the left of the whenchanged attribute.](image)

• The **Event details** page also reflects this change with a blue dot on the left of the whenchanged attribute.
For more details on attributes, see Event Details.

![Event Details](image)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value at event</th>
<th>Current Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>bsdpassword</td>
<td>02/24/2019 22:12:42</td>
<td>02/24/2019 22:12:42</td>
</tr>
<tr>
<td>changed</td>
<td>02/24/2019 22:12:42</td>
<td>02/24/2019 22:12:42</td>
</tr>
<tr>
<td>unchanged</td>
<td>53569</td>
<td>53569</td>
</tr>
<tr>
<td>account</td>
<td>NEVER</td>
<td>NEVER</td>
</tr>
<tr>
<td>cn</td>
<td>MyUser</td>
<td>MyUser</td>
</tr>
<tr>
<td>displayname</td>
<td>MyUser</td>
<td>MyUser</td>
</tr>
<tr>
<td>distinguishedname</td>
<td>CN=MyUser,CN=Users,DC=rsaf,DC=aidsl...</td>
<td>CN=MyUser,CN=Users,DC=rsaf,DC=aidsl...</td>
</tr>
<tr>
<td>instance</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>ntrnsecuritydescriptor</td>
<td>0-5-1-5-29918454942474917</td>
<td>0-5-1-5-29918454942474917</td>
</tr>
<tr>
<td>objectclass</td>
<td>top.person.organizationsPerson</td>
<td>top.org.person.organizationsPerson</td>
</tr>
<tr>
<td>objectguid</td>
<td>0a3e0a5e-29e-0a3e0a5e-1a98f3</td>
<td>0a3e0a5e-29e-0a3e0a5e-1a98f3</td>
</tr>
<tr>
<td>objectid</td>
<td>5-1-2991845494247491763</td>
<td>5-1-2991845494247491763</td>
</tr>
<tr>
<td>primarygroupid</td>
<td>513</td>
<td>513</td>
</tr>
<tr>
<td>samaccountname</td>
<td>poor-little-user</td>
<td>poor-little-user</td>
</tr>
<tr>
<td>samaccounttype</td>
<td>SAM_NORMAL_USER_ACCOUNT</td>
<td>SAM_NORMAL_USER_ACCOUNT</td>
</tr>
<tr>
<td>useraccountcontrol</td>
<td>DONT_EXPIRE NORMAL</td>
<td>DONT_EXPIRE NORMAL</td>
</tr>
<tr>
<td>userprincipalname</td>
<td><a href="mailto:poor-little-user@rsaf.aidsl.co">poor-little-user@rsaf.aidsl.co</a></td>
<td><a href="mailto:poor-little-user@rsaf.aidsl.co">poor-little-user@rsaf.aidsl.co</a></td>
</tr>
</tbody>
</table>
Tenable.ad offers several ways to visualize the potential vulnerability of a business asset through graphical representations.

- **Attack Path**: Shows the possible paths that an attacker can take to compromise an asset from an entry point.
- **Blast Radius**: Shows the possible lateral movements into the Active Directory from any asset.
- **Asset Exposure**: Shows all paths that can potentially take control of an asset.

To display the Attack Path:

1. In Tenable.ad, click **Attack Path** on the sidebar menu. The **Attack Path** pane appears.

2. In the banner, click **Attack Path**.

3. In the **Starting point** box, type the asset at the entry point.

4. In the **Arrival point** box, type the asset at the end of the path.

5. Click the icon.

   Tenable.ad displays the attack path between the two assets.
6. Optionally, you can click on the icon to do the following:

   - Click the **Zoom** slider to adjust the magnification of the graphics.
   - Click the **Show all node tooltips** toggle to display information about the assets.

To display the Blast Radius:

1. In Tenable.ad, click **Attack Path** on the sidebar menu.
   
The **Attack Path** pane appears.

2. In the banner, click **Blast Radius**.

3. In the **Search for an object** box, type the name of an asset.

4. Click the **** icon.

   Tenable.ad displays the lateral connections radiating from that asset:
5. Click on the icons on the arrows between the assets to display the relations between them.

To display the Asset Exposure:

1. To display the Blast Radius:

2. In Tenable.ad, click **Attack Path** on the sidebar menu.

   The **Attack Path** pane appears.

3. In the banner, click **Asset Exposure**.

4. In the **Search for an object** box, type the name of an asset.

5. Click the icon.

   Tenable.ad displays the paths leading to the asset and the relations between the assets.
6. Click on the icons on the arrows between the assets to display the relations between them.

See also

- Attack Relations
Attack Relations

Attack relations are unidirectional from a Source node to a Target node. Since relations are transitive, attackers can chain them together to create an "attack path":

![Tenable.ad](image)

Tenable.ad has the following attack relations:

- Add Key Credential
- Add Member
- Allowed To Act
- Allowed To Delegate
- Belongs To GPO
- DCSync
- Grant Allowed To Act
- Has SID History
- Implicit Takeover
- Inherit GPO
- Linked GPO
- Member Of
- Owns
- Reset Password
• RODC Manage
• Write DACL
• Write Owner
Add Key Credential

Description

The Source security principal can impersonate the Target by exploiting key trust account mappings, also known as key credentials or "shadow credentials".

This is possible because the Source has permission to edit the msDS-KeyCredentialLink attribute of the Target.

Windows Hello for Business (WHfB) normally uses this feature, but it is available for attackers to exploit it even if it is not in use.

Exploitation

Attackers who compromise the Source security principal must edit the msDS-KeyCredentialLink attribute of the Target computer by using specialized hacker tools such as Whisker or DSInternals.

The attackers' goal is to add a new certificate to this target's attribute, for which they have the private key. They can then authenticate as the Target with the known private key using the Kerberos PKINIT protocol to obtain a TGT. This protocol also allows attackers to fetch the target's NTLM hash.

Remediation

Several natively privileged security principals have this permission by default, namely Account Operators, Administrators, Domain Admins, Enterprise Admins, Enterprise Key Admins, Key Admins, and SYSTEM. These legitimate security principals do not require remediation.

For Source security principals without a legitimate need to modify this attribute, you must remove this permission. Search for permissions such as "Write all properties", "Write msDS-AllowedToActOnBehalfOfOtherIdentity", "Full control", etc.

See also

- Add Member
- Allowed To Act
- Allowed To Delegate
- Belongs To GPO
- DCSync
- Grant Allowed To Act
- Has SID History
- Implicit Takeover
- Inherit GPO
- Linked GPO
- Member Of
- Owns
- Reset Password
- RODC Manage
- Write DACL
- Write Owner
Add Member

Description

The Source security principal can add itself (validated write right), or anyone (write property right), to the members of the Target group and benefit from the access rights given to the group.

A malicious security principal performing this operation would create a "Member of" attack relation.

Exploitation

Attackers who compromise the Source security principal only have to edit the "members" attribute of the Target group through native Windows commands such as "net group /domain", PowerShell such as "Add-ADGroupMember", administration tools such as "Active Directory Users and Computers", or dedicated hacker tools such as PowerSploit.

Remediation

If the Source security principal does not need the right to add a member to the Target group, then you must remove this permission.

To modify the security descriptor of the Target group:

2. Remove permissions such as "Write Members", "Write all properties", "Full control", "All validated writes", "Add/remove self as member", etc.

Note: A group can inherit permission from an object higher in the Active Directory tree.

See also

- Add Key Credential
- Allowed To Act
- Allowed To Delegate
- Belongs To GPO
• DCSync
• Grant Allowed To Act
• Has SID History
• Implicit Takeover
• Inherit GPO
• Linked GPO
• Member Of
• Owns
• Reset Password
• RODC Manage
• Write DACL
• Write Owner
Allowed To Act

Description

The Source security principal is allowed to perform Kerberos Resource-Based Constrained Delegation on the Target computer. This means that it can impersonate any user when it authenticates with Kerberos to any service running on the Target computer.

Therefore, it often leads to a total compromise of the Target computer.

This attack is also known as Resource-Based Constrained Delegation (RBCD), Kerberos Resource-Based Constrained Delegation (KRBCD), Resource-Based Kerberos Constrained Delegation (RBKCD), and "allowed to act on behalf of other identity".

Exploitation

Attackers who compromise the Source security principal can use dedicated hacker tools such as Rubeus to exploit legitimate Kerberos protocol extensions (S4U2self and S4U2proxy) in order to forge Kerberos service tickets and impersonate the targeted user. Attackers will likely choose to impersonate a privileged user to obtain privileged access.

Once attackers forge the service ticket, they can use any native administration tool or specialized hacker tool compatible with Kerberos to execute remotely arbitrary commands.

A successful exploitation attempt must meet the following constraints:

- The Source and Target security principals must have a ServicePrincipalName. Tenable.ad does not create this attack relation without this condition.

- The account targeted for spoofing must neither be marked "is sensitive and cannot be delegated" (ADS_UF_NOT_DELEGATED in UserAccountControl) nor be a member of the "Protected Users" group because Active Directory protects such accounts from delegation attacks.

Remediation

If the Source security principal does not need permission to perform Kerberos Resource-Based Constrained Delegation (RBCD) on the Target computer, then you must remove it. You must make the modification on the Target side, as opposed to the "Allowed to delegate" delegation attack relation.
You cannot manage RBCD with existing graphical administration tools such as "Active Directory Users and Computers". You must instead use PowerShell to modify the content of the `msDS-AllowedToActOnBehalfOfOtherIdentity` attribute.

Use the following commands to list the Source security principals allowed to act on the Target (in the "Access:" section):

```powershell
Get-ADComputer target -Properties msDS-AllowedToActOnBehalfOfOtherIdentity | Select-Object -ExpandProperty msDS-AllowedToActOnBehalfOfOtherIdentity | Format-List
```

If you do not want any of the listed security principals is desired, you can clear all of them with this command:

```powershell
Set-ADComputer target -Clear "msDS-AllowedToActOnBehalfOfOtherIdentity"
```

If you only need to remove one security principal from the list, Microsoft unfortunately does not provide a direct command. You must overwrite the attribute with the same list minus the one to remove. For example, if "sourceA", "sourceB" and "sourceC" were all allowed and you want to remove just "sourceB", run:

```powershell
Set-ADComputer target -PrincipalsAllowedToDelegateToAccount (Get-ADUser sourceA),(Get-ADUser sourceC)
```

Finally, as a general recommendation, in order to limit the exposure of sensitive privileged accounts to such delegation attacks, Tenable.ad recommends that you mark them as "is sensitive and cannot be delegated" (ADS_UF_NOT_DELEGATED) or add them to the "Protected Users" group, after careful verification of the associated operational impacts.

See also

- [Add Key Credential](#)
- [Add Member](#)
- [Allowed To Delegate](#)
- [Belongs To GPO](#)
- [DCSync](#)
• Grant Allowed To Act
• Has SID History
• Implicit Takeover
• Inherit GPO
• Linked GPO
• Member Of
• Owns
• Reset Password
• RODC Manage
• Write DACL
• Write Owner
Allowed To Deleg ate

Description

The Source security principal is allowed to perform Kerberos Constrained Delegation (KCD) with protocol transition on the Target computer. This means that it can impersonate any user when it authenticates with Kerberos to any service running on the Target computer.

Therefore, it often leads to a total compromise of the Target computer.

Exploitation

Attackers who compromise the Source security principal can use dedicated hacker tools such as Rubeus to exploit legitimate Kerberos protocol extensions (S4U2self and S4U2proxy) in order to forge Kerberos service tickets and impersonate the targeted user. Attackers are likely to choose to impersonate a privileged user to obtain privileged access.

Once attackers forge the service ticket, they can use any native administration tool or specialized hacker tool compatible with Kerberos to execute remotely arbitrary commands.

A successful exploitation attempt must meet the following constraints:

- The Source security principal must be enabled for protocol transition (ADS_UF_TRUSTED_TO_AUTHENTICATE_FOR_DELEGATION in UserAccountControl / "Use any authentication protocol" in the Delegation GUI). More precisely, the attack could work without protocol transition ("Use Kerberos only" in the Delegation GUI), but attackers must first coerce a Kerberos authentication from the targeted user to the Source security principal, which makes the attack harder. Therefore, Tenable.ad does not create an attack relation in this case.

- The Source and Target security principals must have a ServicePrincipalName. Tenable.ad does not create this attack relation without this condition.

- The account targeted for spoofing must neither be marked "is sensitive and cannot be delegated" (ADS_UF_NOT_DELEGATED in UserAccountControl) nor be a member of the "Protected Users" group because Active Directory protects such accounts from delegation attacks.

On the contrary, the Target computer where delegation is allowed is designated by a Service Principal Name (SPN) and thus contains a specific service such as SMB with "cifs/host.example.net", HTTP with "http/host.example.net", etc. However, attackers can actually target any other SPN and
service running under the same Target account using a "sname substitution attack". Therefore, this is not a limitation.

Remediation

If the Source security principal does not need permission to perform Kerberos Constrained Delegation (KCD) on the Target computer, then you must remove it. You must make the modification on the Source side, as opposed to an "Allowed to act" delegation attack relation.

To remove the Source security principal:

1. In "Active Directory Users and Computers" administration GUI, go to the Source object's Properties > Delegation tab.
2. Remove the Service Principal Name corresponding to the Target.
3. If you do not want any delegation from this Source, remove all SPNs and select "Do not trust this computer for delegation".

Alternatively, you can use PowerShell to modify the content of the Source's "msDS-AllowedToDelegateTo" attribute.

- For example, in Powershell, run this command to replace all values:

  ```powershell
  Set-ADObject -Identity "CN=Source,OU=corp,DC=example,DC=net" -Replace @"{"msDS-AllowedToDelegateTo" = @("cifs/desiredTarget.example.net") }"
  ```

- If you do not want any delegation from this Source, run the following command to clear the attribute:

  ```powershell
  Set-ADObject -Identity "CN=Source,OU=corp,DC=example,DC=net" -Clear "msDS-AllowedToDelegateTo"
  ```

It is also possible to reduce the risk while not completely closing this attack path by disabling protocol transition. This requires that all security principals connect to the Source using only Kerberos instead of NTLM.

To disable protocol transition:
1. In "Active Directory Users and Computers" administration GUI, go to the Source object's Properties > Delegation tab.

2. Select "Use Kerberos only" instead of "Use any authentication protocol".

Alternatively, you can run the following command in PowerShell to disable protocol transition:

```
Set-ADAccountControl -Identity "CN=Source,OU=corp,DC=example,DC=net" -TrustedToAuthForDelegation $false
```

Finally, as a general recommendation, in order to limit the exposure of sensitive privileged accounts to such delegation attacks, Tenable.ad recommends that you mark them as "Is sensitive and cannot be delegated" (ADS_UF_NOT_DELEGATED) or add them to the "Protected Users" group after careful verification of the associated operational impacts.

See also

- Add Key Credential
- Add Member
- Allowed To Act
-Belongs To GPO
-DCSync
-Grant Allowed To Act
-Has SID History
-Implicit Takeover
-Inherit GPO
-Linked GPO
-Member Of
-Owns
-Reset Password
• RODC Manage

• Write DACL

• Write Owner
Belongs To GPO

Description
The Source GPO file or folder in the SYSVOL share belongs to the target GPC (GPO), which means that it defines the settings or programs/scripts that the GPO applies.

Exploitation
This is not an attack relation that an attacker would use in isolation. However, as an example, it can show complete attack paths where attackers who have control over a GPO file/folder belonging to a GPO can force arbitrary settings or launch scripts on the users/computers at the end of the attack path.

Remediation
This relation shows how GPO files and folders found in SYSVOL are related to the corresponding GPC (GPO) object. This is normal and by design.

Therefore, there is no need for remediation.

See also
- Add Key Credential
- Add Member
- Allowed To Act
- Allowed To Delegate
- DCSync
- Grant Allowed To Act
- Has SID History
- Implicit Takeover
- Inherit GPO
- Linked GPO
- Member Of
- Owns
- Reset Password
- RODC Manage
- Write DACL
- Write Owner
DCSync

Description

DCSync is a legitimate Active Directory feature that domain controllers only use for replicating changes, but illegitimate security principals can also use it.

The Source security principal can request sensitive secrets (password hashes, Kerberos keys, etc.) from the Target domain using the DCSync feature, ultimately leading to a total compromise of the domain.

To fetch secrets, two security permissions are required: "Replicating Directory Changes" (DS-Replication-Get-Changes) and "Replicating Directory Changes All" (DS-Replication-Get-Changes-All). The relation occurs only if you give both of these permissions to the Source, either directly or through nested group membership.

Exploitation

Attackers who compromise the Source security principal can fetch secrets using dedicated hacker tools such as mimikatz or impacket.

- **Golden ticket**: Results from obtaining the password hash of the "krbtgt" account, which makes it possible to forge a Kerberos TGT and allows the impersonation of anyone on any computer/service. This notably gives administrative privileges over any computer in the domain.

- **Silver ticket**: Results from obtaining the password hash of a computer/service account, which makes it possible to forge a Kerberos service ticket and allows the impersonation of anyone on the given computer/service.

Remediation

Legitimate security principals allowed by default to leverage DCSync are:

- Administrators
- Domain Admins
- Enterprise Admins
- SYSTEM
In addition, the Azure AD Connect configuration allows its password hash synchronization service account (MSOL_...) to leverage DCSync.

Finally, it is possible to discover service accounts for certain security tools, notably password auditing solutions. Verify their legitimacy with the people in charge.

For Source security principals without a legitimate need to perform DCSync, you must remove this permission.

To modify the security descriptor of the Target domain:

1. In "Active Directory Users and Computers", right-click the domain name and select Properties > Security.

2. Remove the "Replicating Directory Changes" and "Replicating Directory Changes All" permissions for illegitimate security principals.

**Note:** DCSync relations can occur through permissions from nested group membership. Hence depending on the exact situation, you must remove the groups themselves or only some of their members.

See also

- [Add Key Credential](#)
- [Add Member](#)
- [Allowed To Act](#)
- [Allowed To Delegate](#)
- [Belongs To GPO](#)
- [Grant Allowed To Act](#)
- [Has SID History](#)
- [Implicit Takeover](#)
- [Inherit GPO](#)
- [Linked GPO](#)
- [Member Of](#)
- Owns
- Reset Password
- RODC Manage
- Write DACL
- Write Owner
Grant Allowed To Act

Description

The Source security principal is allowed to grant itself or someone else an Allowed To Act relation to the Target computer. It often leads to a total compromise of the Target computer via a Kerberos RBCD delegation attack.

This is possible because the Source has the permission to edit the Target's "msDS-AllowedToActOnBehalfOfOtherIdentity" attribute.

A malicious security principal performing this operation can create an "Allowed To Act" attack relation.

Exploitation

Attackers who compromise the Source security principal must edit the Target computer's msDS-AllowedToActOnBehalfOfOtherIdentity attribute using PowerShell (for example "Set-ADComputer <target> -PrincipalsAllowedToDelegateToAccount ...").

Remediation

Several natively privileged security principals have this permission by default, namely Account Operators, Administrators, Domain Admins, Enterprise Admins and SYSTEM. These security principals are legitimate and do not require remediation.

Kerberos RBCD is designed so that a computer's administrators can give the rights to perform delegation on the computer to anyone who needs it. This is different from other modes of Kerberos delegation that require Domain Admins level permission. This allows lower-level administrators to manage these security settings themselves, which is a principle also called delegation. In this case, the relation is legitimate.

However, if the Source security principal is not a legitimate administrator of the Target computer, the relation is not legitimate and you must remove this permission.

To modify the security descriptor of the Target computer:

2. Remove the permission given to the Source security principal. Look for permissions such as "Write msDS-AllowedToActOnBehalfOfOtherIdentity", "Write all properties", "Write account restrictions", "Full control", etc.

**Note:** The Source security principal can inherit the permission from an object higher in the Active Directory tree.

See also

- Add Key Credential
- Add Member
- Allowed To Act
- Allowed To Delegate
- Belongs To GPO
- DCSync
- Has SID History
- Implicit Takeover
- Inherit GPO
- Linked GPO
- Member Of
- Owns
- Reset Password
- RODC Manage
- Write DACL
- Write Owner
Has SID History

Description

The Source security principal has the SID of the Target security principal in its SIDHistory attribute, which means that the Source has the same rights as the Target.

SID History is a legitimate mechanism used when migrating security principals between domains to keep all authorizations referencing their previous SID functional.

However, this is also a persistence mechanism that attackers use, as it allows a discreet backdoor account to have the same rights as the desired target such as an Administrator account.

Exploitation

Attackers who compromise the Source security principal can directly authenticate as the Target security principal since the Target's SID is transparently added into the token that Active Directory authentication mechanisms generate (NTLM & Kerberos).

Remediation

If the Source and Target security principals are related to an approved domain migration, you can consider the relation to be legitimate and not perform any action. This relation remains visible as a reminder of a potential attack path.

If the domain of origin was deleted after the migration or is not configured in Tenable.ad, the Target security principal is marked as unresolved. Since the risk lies with the Target and that Target does not exist, there is no risk and hence no remediation required.

On the contrary, SID History relations to natively privileged users or groups are very likely malicious since Active Directory prevents their creation. This means that they were probably created using hacker techniques such as a "DCShadow" attack. You can also find these cases in the IoE related to "SID History".

If this is the case, Tenable.ad recommends a forensic examination of the entire Active Directory forest. The reason is that attackers must have obtained high privileges – domain administrator or equivalent – to edit maliciously the Source's SID history. The forensic examination helps you ana-
lyze the attack with corresponding remediation guidance, and identifies potential backdoors to remove.

Finally, Microsoft recommends that you modify all access rights in all services (SMB shares, Exchange, etc.) to use the new SIDs and remove unnecessary SIDHistory values after this migration is complete. This is a housekeeping best practice, although identifying exhaustively and fixing all ACLs is very difficult.

A user who has the right to edit the SIDHistory attribute on the Source object itself can remove SIDHistory values. Contrary to creation, this operation does not require domain administrator rights.

To do this, you can only use PowerShell because graphical tools such as Active Directory Users and Computers will fail. Example:

```
Set-ADUser -Identity <user> -Remove @{sidhistory="S-1-..."}
```

Caution: While removing a SIDHistory value is easy, reverting this operation is very complicated. This is because you must recreate the SIDHistory value which requires the presence of the other domain that may be decommissioned. For this reason, Microsoft also recommends that you prepare snapshots or backups.

See also

- Add Key Credential
- Add Member
- Allowed To Act
- Allowed To Delegate
- Belongs To GPO
- DCSync
- Grant Allowed To Act
- Implicit Takeover
- Inherit GPO
- Linked GPO
• Member Of
• Owns
• Reset Password
• RODC Manage
• Write DACL
• Write Owner
Implicit Takeover

Description

The Source is a Tier0 security principal. Tier0 is the set of Active Directory objects that have the highest privileges in the domain, such as the members of the Domain Admins or Domain Controllers group. All Tier0 assets can implicitly compromise any other object in the domain, even if there is no explicit other relation.

This relation makes it possible to model implicit rights built-in to Active Directory. These rights are by design and documented, and thus known to attackers. However, Tenable.ad cannot collect these rights by standard means. Moreover, this relation simplifies attack path graphs, because as soon as attackers compromise a Tier0 node, they can attack any other object directly without going through other explicit relations.

In summary, Source Tier0 assets are considered to all have "Implicit Takeover" relations to any Target node in the graph.

Exploitation

The exact exploitation method depends on the type of the Source Tier0 asset targeted, but these are well-documented techniques that attackers efficiently master.

Remediation

This relation is by design and you cannot remediate it. It is almost impossible to stop an attacker who reaches a Tier0 asset from attacking further.

Remediation efforts must focus on upstream relations in attack paths.

See also

- Add Key Credential
- Add Member
- Allowed To Act
- Allowed To Delegate
- Belongs To GPO
- DCSync
- Grant Allowed To Act
- Has SID History
- Inherit GPO
- Linked GPO
- Member Of
- Owns
- Reset Password
- RODC Manage
- Write DACL
- Write Owner
Inherit GPO

Description

A Source linkable container such as an Organizational Unit (OU) or Domain - but not Sites - contains the Target OU, User, Device, DC, or Read-Only Domain Controller (RODC) in the LDAP tree. This is because the children objects of the linkable container inherit the GPO where it is linked (see "Linked GPO" relations).

Tenable.ad takes into account whenever an OU blocks inheritance.

Exploitation

Attackers have nothing to do to exploit this relation as long as they manage to compromise the GPO upstream in the attack path. By design, the relation applies to linkable containers and objects below them, as shown by Inherit GPO relations.

Remediation

In most cases, it is normal and legitimate for GPOs to apply to linkable children containers from their parent containers. However, this linkage exposes additional attack paths.

Therefore, in order to reduce risks, you should link GPOs to the lowest level in the organizational units hierarchy, whenever possible.

Moreover, GPOs require protection from unauthorized modifications by attackers, in order not to expose them to other attack relations.

Finally, OUs can disable GPO inheritance from higher levels through their "block inheritance" option. However, use this option only as a last resort because it blocks all GPOs -- including the potential security hardening GPOs defined at the highest domain level. It also makes the reasoning about applied GPOs more difficult.

See also

- Add Key Credential
- Add Member
• Allowed To Act
• Allowed To Delegate
• Belongs To GPO
• DCSync
• Grant Allowed To Act
• Has SID History
• Implicit Takeover
• Linked GPO
• Member Of
• Owns
• Reset Password
• RODC Manage
• Write DACL
• Write Owner
Linked GPO

Description

The Source GPO is linked to the Target linkable container, such as a Domain or Organizational Unit (OU). This means that the Source GPO can assign settings and run programs on the devices and users contained in the Target. The Source GPO also applies to objects in containers below it through "Inherit GPO" relations.

Ultimately, the GPO can compromise the devices and users on which it applies.

Exploitation

Attackers must first compromise the Source GPO through another attack relation.

From there, they employ several techniques to perform malicious actions on devices and users contained in the Target and those below it. Examples are:

- Abusing the legitimate "immediate scheduled tasks" to execute arbitrary scripts on devices.
- Adding a new local user with administrative rights on all devices
- Installing an MSI program
- Disabling the firewall or antivirus
- Granting further rights
- etc.

Attackers can modify a GPO by manually editing its content using administration tools such as "Group Policy Management" or dedicated hacker tools such as PowerSploit.

Remediation

In most cases, linking a GPO to a linkable container is normal and legitimate. However, this linkage increases the attack surface where it occurs as well as in the containers below it.

Therefore, in order to reduce risks, you should link GPOs to the lowest level in the organizational units hierarchy, whenever possible.
Moreover, GPOs require protection from unauthorized modifications by attackers, in order not to expose them to other attack relations.

See also

- [Add Key Credential](#)
- [Add Member](#)
- [Allowed To Act](#)
- [Allowed To Delegate](#)
- [Belongs To GPO](#)
- [DCSync](#)
- [Grant Allowed To Act](#)
- [Has SID History](#)
- [Implicit Takeover](#)
- [Inherit GPO](#)
- [Member Of](#)
- [Owns](#)
- [Reset Password](#)
- [RODC Manage](#)
- [Write DACL](#)
- [Write Owner](#)
Member Of

Description

The Source security principal is a member of the Target group. Therefore, it benefits from all the access rights that the group holds, such as accessing file shares, assuming roles in business applications, etc.

Exploitation

Attackers do not have to do anything to exploit this attack relation. They only need to authenticate as the Source security principal to get the Target group in their local or remote security token, or Kerberos ticket.

Remediation

If the Source security principal is an illegitimate member of the Target group, then you must remove it.

You can use any standard Active Directory administration tool such as "Active Directory Users and Computers" or PowerShell such as Remove-ADGroupMember.

See also

- Add Key Credential
- Add Member
- Allowed To Act
- Allowed To Delegate
- Belongs To GPO
- DCSync
- Grant Allowed To Act
- Has SID History
• Implicit Takeover
• Inherit GPO
• Linked GPO
• Owns
• Reset Password
• RODC Manage
• Write DACL
• Write Owner
Owns

Description

The Source security principal is the declared owner of the Target object because it likely created the Target object. Owners have implicit rights - "Read Control" and "Write DACL" - that allow them to obtain additional rights, for themselves or someone else, and ultimately compromise the Target object.

Exploitation

Attackers who compromise the Source security principal only have to edit the Target object's security descriptor using native Windows commands such as "dsacls", PowerShell such as "Set-ACL", administration tools such as "Active Directory Users and Computers", or dedicated hacker tools such as PowerSploit.

When an object gets created, there is a risk of privilege escalation if a low privileged user creates it and thus owns it - for example, a standard helpdesk technician - and later that object gets elevated to higher privileges - for example, administrator. The original owner remains and can now compromise the newly privileged object to take advantage of its privileges.

Remediation

If the Source security principal is not a legitimate owner of the Target object, then you must change it.

To change the owner of the Target object:

2. On the Owner line at the top, click Change.

Safe Target object owners used by default for most sensitive Active Directory objects are:

- Objects in the Domain partition: "Administrators" or "Domain Admins"
- Objects in the Configuration partition: "Enterprise Admins"
- Objects in the Schema partition: "Schema Admins"
See also

- Add Key Credential
- Add Member
- Allowed To Act
- Allowed To Delegate
- Belongs To GPO
- DCSync
- Grant Allowed To Act
- Has SID History
- Implicit Takeover
- Inherit GPO
- Linked GPO
- Member Of
- Reset Password
- RODC Manage
- Write DACL
- Write Owner
Reset Password

Description

The Source security principal can reset the password of the Target, which allows it to authenticate as the Target using the new attributed password and benefit from the Target's privileges.

Resetting a password is not the same as changing a password, which anyone who knows the current password can do. A password change typically occurs when a password expires.

Exploitation

Attackers who compromise the Source security principal can reset the password of the Target using native Windows commands such as "net user /domain", PowerShell such as "Set-ADAccountPassword -Reset", administration tools such as "Active Directory Users and Computers", or dedicated hacker tools such as PowerSploit.

Attackers then only have to authenticate to the Active Directory or the targeted resource using legitimate authentication methods with their new chosen password to impersonate fully the Target.

However, attackers do not usually know the previous password to revert to it after the attack. Therefore, the attack is often visible for the legitimate person behind the Target and can even cause a denial of service, especially for service accounts.

Remediation

IT administrators and helpdesk staff are legitimately allowed to reset passwords. But you must put in place the appropriate delegations to let them perform this action only within their allowed perimeter.

Also, according to the tiering model, you must ensure that a lower level staff such as a helpdesk for normal users cannot reset the password of a higher level account, such as a domain administrator, because this is an opportunity for privilege escalation.

To modify the Target's security descriptor and remove illegitimate permissions:

2. Remove "Reset password" permission for the Source security principal.
Note: Do not confuse this permission with "Change password".

See also

- Add Key Credential
- Add Member
- Allowed To Act
- Allowed To Delegate
- Belongs To GPO
- DCSync
- Grant Allowed To Act
- Has SID History
- Implicit Takeover
- Inherit GPO
- Linked GPO
- Member Of
- Owns
- RODC Manage
- Write DACL
- Write Owner
RODC Manage

Description

The Source security principal is found in the "ManagedBy" attribute of the Target Read-Only Domain Controller (RODC). This means that the Source has administrative rights over the Target RODC.

**Note**: Other Active Directory object types use the same "ManagedBy" attribute for informational purposes only, and do not give any administrative rights to the declared manager. Therefore, this relation exists only for Target nodes of the RODC type.

RODCs are less sensitive than the more common writable Domain Controllers, but they are still a high-value target for attackers because they can steal credentials from RODCs to allow them to pivot further to other systems. This depends on the level of hardening in the RODC's configuration - for example, the number of objects with secrets that it can synchronize.

Exploitation

The exploitation method is identical to that of the "AdminTo" relation.

Attackers who compromise the Source security principal can use its identity to connect remotely and execute commands on the Target RODC with administrative rights. They can exploit available native protocols such as Server Message Block (SMB) with administrative shares, Remote Desktop Protocol (RDP), Windows Management Instrumentation (WMI), Remote Procedure Call (RPC), Windows Remote Management (WinRM), etc.

Attackers can use native remote administration tools such as PsExec, services, scheduled tasks, Invoke-Command, etc., or specialized hacker tools such as wmiexec, smbexec, Invoke-DCOM, SharpRDP, etc.

The attack's final goal can either be to compromise the Target RODC or to use credential dumping tools such as mimikatz to obtain more credentials and secrets to pivot to other machines.

Remediation

If the Source security principal is not a legitimate administrator of the Target Read-Only Domain Controller (RODC), then you must replace it with a proper administrator.
Note that Domain Admins do not generally administer RODCs, hence the dedicated "managed by" setting. This is because RODCs have a lower trust level and high-privileged Domain Admins should not expose their credentials by authenticating on them.

Therefore, you must select a proper "middle-level" administrator for RODCs according to your Active Directory RODC rules - for example, the IT administrator of an organization's local branch where they are located.

To change the "ManagedBy" attribute:

1. In "Active Directory Users and Computers", select the RODC > Properties > "ManagedBy" tab.
2. Click Change.

You can also run the following command in PowerShell:

```
Set-ADComputer <rodc> -ManagedBy (Get-ADUser <rodc_admin>)
```

See also

- Add Key Credential
- Add Member
- Allowed To Act
- Allowed To Delegate
- Belongs To GPO
- DCSync
- Grant Allowed To Act
- Has SID History
- Implicit Takeover
- Inherit GPO
- Linked GPO
• Member Of
• Owns
• Reset Password
• Write DACL
• Write Owner
Write DACL

Description

The Source security principal has the permission to change the permissions of the Target object in the Discretionary Access Control List (DACL). This allows the Source to obtain for themselves, or give to someone else, additional rights and ultimately compromise the Target object.

Exploitation

Attackers who compromise the Source security principal only have to edit the Target object's security descriptor using native Windows commands such as "dsacl", PowerShell such as "Set-ACL", administration tools such as "Active Directory Users and Computers", or dedicated hacker tools such as PowerSploit.

Remediation

If the Source security principal does not have legitimate permission to change the permissions of the Target object, then you must remove this permission.

To modify the Target object's security descriptor:

1. In "Active Directory Users and Computers", right-click the object then Properties > Security > Advanced.

2. Remove the "Modify permissions" permission for the Source security principal.

Note: An object can inherit this permission from an object higher in the Active Directory tree.

See also

- Add Key Credential
- Add Member
- Allowed To Act
- Allowed To Delegate
• Belongs To GPO
• DCSync
• Grant Allowed To Act
• Has SID History
• Implicit Takeover
• Inherit GPO
• Linked GPO
• Member Of
• Owns
• Reset Password
• RODC Manage
• Write Owner
Write Owner

Description

The Source security principal has the permission to change the owner of the Target object, including assigning themselves as the owner. Owners have implicit rights, "Read Control" and "Write DACL", that allow them to obtain additional rights for themselves or for someone else, and ultimately compromise the Target object.

For more information, see the Owns relation.

Exploitation

Attackers who compromise the Source security principal can assign themselves as the owner of the Target using native Windows commands such as "dsacls /takeownership", PowerShell such as "Set-ACL", administration tools such as "Active Directory Users and Computers", or dedicated hacker tools such as PowerSploit.

They can then edit the Target object's security descriptor using similar methods.

Remediation

If the Source security principal does not have legitimate permission to change the Target object's owner, then you must remove this permission.

To modify the Target object's security descriptor:

1. In "Active Directory Users and Computers", right-click the object and select **Properties > Security > Advanced**.

2. Remove the "Modify owner" permission for the Source security principal.

**Note:** An object can inherit this permission from an object higher in the Active Directory tree.

See also
- Add Key Credential
- Add Member
- Allowed To Act
- Allowed To Delegate
- Belongs To GPO
- DCSync
- Grant Allowed To Act
- Has SID History
- Implicit Takeover
- Inherit GPO
- Linked GPO
- Member Of
- Owns
- Reset Password
- RODC Manage
- Write DACL
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).

Chart types: line & 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 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:

![Image of Tenable Ad interface with multiple domains and attack indicators]

• Show only domains under attack enabled:

![Image of Tenable Ad interface with highlighted domains and attack indicators]
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

![Image of a timeline interface]

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.
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
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.

*Interactive elements (IoE page)*
Clickable entries

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

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

Toggle switches

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

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

Blades (also called tabs)

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

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

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

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

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

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

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

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

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

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

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

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

Display Mode

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

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

Severity Levels

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

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

**Tile Information**

Each IoE tile displays the following information:

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

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

Purpose

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

Search for an Indicator

Indicators of Exposure can be displayed:

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

Examples

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

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

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

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

**Critical**

- Weak password policies are applied on users
  - Some password policies applied on specific user accounts are not strong enough and can lead to credentials theft.
  - Tenable's domain

**High**

- Potential clear-text password
  - Some clear-text passwords seem to be readable by every domain's users
  - Tenable's domain

**Medium**

- Accounts with never expiring passwords
  - Accounts with the DONT_EXPIRE property are not affected by password renewal policy
  - Tenable's domain

**Low**

- No indicators found with deviant objects
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.

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

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

**Lower section**

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

![Image of clickable blades](image-url)
Indicator of Exposure details

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

View Information Blade

This blade includes the following sub-sections:

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

View Vulnerability Details Blade

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

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

Purpose

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

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

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

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

**Blade layout**

This blade includes the following items:

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

**Understand table labels**

The deviant objects table includes the following items:

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

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

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

View Recommendations Blade

Purpose

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

Blade layout
This blade includes the following sub-sections:

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

**Recommendations blade**

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

Purpose

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

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

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

Locate Data

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

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

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

Wizard search

Search elements in the wizard

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

**AND/OR combinator buttons**

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

Search elements in the wizard

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

Add a new condition

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

Add a new rule

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

Query syntax

Add an attribute

1. After applying the combinator to the first condition, select the attribute from the dropdown menu and enter its value.
2. Click on the +Add a new rule action button to add another attribute to the first condition.
3. If you add another condition to the query, click on the +AND or +OR combinator button.

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.

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.

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.
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 `krb5_kdc` account is privileged (`CN=Administrators,CN=Global,CN=Users,DC=example,DC=corp`) but is not part of the Protected Users group nor has the `not_delegable` 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 `krb5_kdc` 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.
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 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 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 account:

1. In Tenable.ad, 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>
</table>
| Enabled                  | • **Enabled**— Tenable.ad blocks the account after a set number of failed login attempts.  
                            • **Disabled**— Tenable.ad does not lock the account after failed login attempts. | Enabled       |
| Lockout duration         | 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.  
                            To configure the lockout duration:  
                            1. Click on the slider to set a lockout duration.  
                            2. Select **Infinite** if you do not want to unlock the account automatically after a set duration. | 300 seconds   |
| Number of attempts before lockout | The number of failed login attempts before Tenable.ad locks the account. | 3             |
| Redemption period        | 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.  
                            To set the redemption period:  
                            1. Click on the slider to set a time interval.  
                            2. Select "Infinite" if you do not want to set a time interval to count unsuccessful login attempts before Tenable.ad locks the account. | 900 seconds   |
6. Click **Save**.

To disable the lockout policy:

1. In Tenable.ad, 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 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 updated the user's permissions.

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

Tenable.ad allows you to authenticate using Lightweight Directory Access Protocol (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, 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 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 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, 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 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 uses to grant access to in the Tenable.ad 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, 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 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 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 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 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 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 only accepts alphanumeric characters and underscores.

5. Click the **Create** button in the lower-right corner.
   
   A message indicates that Tenable.ad 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 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, 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 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".

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
7. Click **Save as draft**.

   A message confirms that Tenable.ad 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 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 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 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, 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 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, 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 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, 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 updated the role.

To set permissions in bulk for a role:
1. In Tenable.ad, 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 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 Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Edit</strong></td>
<td>Permission to modify an object or a configuration. Requires the Read permission to apply modifications.</td>
</tr>
<tr>
<td><strong>Create</strong></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 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>
</table>
| **Data Entities** | This entity controls the permissions for setting up the monitored Active Directory and configuring the data analysis in Tenable.ad. | • Indicators of Attack  
• Indicators of Exposure  
• Forests  
• Domains  
• Profiles  
• Users  
• Alerts by email  
• Alerts by Syslog  
• Roles | Read, Edit, Create |

| **User Entities** | | Edit, Create |
| This entity controls a user's ability to configure information that Tenable.ad displays for data analysis and to modify personal information and preferences. | • Preferences  
• Dashboards  
• Widgets  
• API key |
<table>
<thead>
<tr>
<th>System Configuration Entities</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>This entity controls the access to the Tenable.ad platform and services.</td>
<td>Application services (SMTP, logs, authentication Tenable.ad, Indicators of Attack, PKI settings)</td>
</tr>
<tr>
<td></td>
<td>Scores through public API</td>
</tr>
<tr>
<td></td>
<td>Licences</td>
</tr>
<tr>
<td></td>
<td>LDAP authentication</td>
</tr>
<tr>
<td></td>
<td>SAML authentication</td>
</tr>
<tr>
<td></td>
<td>Topology</td>
</tr>
<tr>
<td></td>
<td>Accounts Lockout Policy</td>
</tr>
<tr>
<td></td>
<td>Recrawl domains</td>
</tr>
<tr>
<td></td>
<td>Change the max IOA workload quota</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface Entities</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>This entity defines the permissions to access specific parts of the Tenable.ad user interface and features.</td>
<td>Access paths to specific Tenable.ad features. For more information, see <a href="example">Set Permissions on User Interface Entities (Example)</a>.</td>
</tr>
<tr>
<td></td>
<td>Granted, Unauthorized</td>
</tr>
</tbody>
</table>

See also

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

Tenable.ad 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:

- 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, 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 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 implicitly grants the Read and Edit permissions.

9. Click Apply and Close.

   A message confirms that Tenable.ad updated permissions on the entities.
Forests

To add a forest:

1. In Tenable.ad, 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 uses:
   - Login
   - Password
5. Click Add.
   A message confirms the addition a new forest.

To edit a forest:

1. In Tenable.ad, 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 updated the forest.
Domains

Tenable.ad 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:

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

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 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:

1. In Tenable.ad, click **Systems**.
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 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:

1. In Tenable.ad, click Systems.
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 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:

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

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’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, 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 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 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 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 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 may take some time to process and activate the Honey Account.

**To edit a Honey Account:**

1. In Tenable.ad, 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 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 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.
To delete a Honey Account:

1. In Tenable.ad, 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 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, 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 clears the activity status of each attack after you save the configuration.

6. Click **Confirm**.

   A message confirms that Tenable.ad 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.

![Powershell](image)

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

```powershell
./Register-TenableIDA.ps1 -ControllerAddress 10.109.6.26 -TenableServiceAccount dcdefn
./Register-TenableIDA.ps1 -ControllerAddress 10.109.6.10 -TenableServiceAccount alejiodcdefn
```

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 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, 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 updated the quota maximum limit.

5. Click **Save**.

   A confirmation message informs you that Tenable.ad clears the activity status of each attack after you save the configuration.

6. Click **Confirm**.

   A message confirms that Tenable.ad 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)

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

```
./Register-TenableIDa.ps1 -DomainControllerAddress 10.108.6.26 -TenableServiceAccount dcdefn
./Register-TenableIDa.ps1 -DomainControllerAddress 10.108.6.10 -TenableServiceAccount aleu1dcdefn
```

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'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
- Domain Backup Key Extraction
- Enumeration of Local Administrators
- GoldenTicket
- Kerberasting
- 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](#)
- [Domain Backup Key Extraction](#)
• Enumeration of Local Administrators
• GoldenTicket
• Kerberoasting
• Massive Computers Reconnaissance
• NTDS Extraction
• Password Guessing
• Password Spraying
• PetitPotam
DCShadow

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

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

Requires Sysmon extension

No

See also

- [Credential Dumping: LSASS Memory](#)
- [DCSync](#)
- [Domain Backup Key Extraction](#)
- [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.

### 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</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](#)
- [Domain Backup Key Extraction](#)
- [Enumeration of Local Administrators](#)
- [GoldenTicket](#)
- [Kerberoasting](#)
- [Massive Computers Reconnaissance](#)
- [NTDS Extraction](#)
- [Password Guessing](#)
- [Password Spraying](#)
- [PetitPotam](#)
Domain Backup Key Extraction

The Data Protection API (DPAPI) helps to protect data in operating systems running Windows 2000 and later. Operating systems and applications use DPAPI to protect private keys, stored credentials in Windows XP and later, and other information that they want to keep confidential.

DPAPI uses a mechanism involving several keys created for users and computers objects. For example, when a user logs on to a computer the first time, the system creates a key derived from the user’s password that encrypts the first copy of the user’s DPAPI master key. The system stores these master keys in the directory C:\User-s\<USER>\AppData\Roaming\Microsoft\Protect\<SID>\<GUID>, where <SID> is the user’s security identifier and <GUID> is the name of the master key.

**Note:** The system stores DPAPI computers keys in the system profile directory.

The decrypting of the master key requires the user or computer password. In order to support password resets, the system encrypts a secondary copy of the master key with a DPAPI Domain Backup Key and replicates it on all writable domain controllers. Since this DPAPI Domain Backup Key is global to the domain, any compromise by an attacker can give access to any encrypted confidential data using the DPAPI mechanism.

Examples of DPAPI secrets:

- User
  - Windows “Credentials” (like saved RDP creds)
  - Windows Vaults
  - Saved IE and Chrome logins/cookies
  - Remote Desktop Connection Manager files with passwords
  - Dropbox syncs

- System
- Scheduled tasks credentials
- Azure sync accounts
- Wifi credentials

<table>
<thead>
<tr>
<th>Detection Type</th>
<th>Related to a Common Vulnerabilities and Exposures (CVE)</th>
<th>Available from Tenable.ad version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic IOC</td>
<td>No</td>
<td>3.17</td>
</tr>
</tbody>
</table>

**How the attack works**

The attacker must be a privileged user on the domain to perform the correct Local Security Authority (LSA) RPC calls to extract the DPAPI Domain Backup Key. The system stores this domain backup key using an LSA secret object and generates audit events when accessed.

To achieve this extraction, common attack tools like *mimikatz* carry out the following steps:

1. Logs on to the Domain Controller (DC).
2. Accesses the named pipe "lsarpc" to communicate with the LSA functions.
3. Gets a handle on the global LSA secret object named G$BCKUPKEY_PREFERRED and reads it. It contains the GUID of the actual used Domain Backup Key.
4. Gets a handle on the global LSA secret object named G$BCKUPKEY_<GUID> (e.g. G$BCKUPKEY_935e526e-e44b-4032-9355-265b57c7dea2) and reads it. It contains the actual Domain Backup Key used.
5. Returns the private key of the Domain Backup Key pair.

Once attackers obtain this private key, they can decrypt any DPAPI secrets on the domain.

**How the IoA works**

The DPAPI Domain Backup Key Extraction Indicator of Attack can detect a wide variety of attack tools that use LSA RPC calls to access backup keys.

The strategy is to identify specific patterns in Active Directory events that relate to the access of LSA secret objects containing sensitive data in DPAPI keys. Since certain tools access both current mod-

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
ern and legacy keys, the Indicator of Attack does not raise multiple deviations for the same attack scenario.

By using enrichment events, the IoA can also provide a detailed description of a DPAPI Domain Backup Key extraction attack.

**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></td>
<td></td>
<td></td>
<td>└ Sub-category: Audit Directory Service Access</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**

- Sysmon extension: No
- Honey Account: No

**See also**

- [Credential Dumping: LSASS Memory](#)
- [DCShadow](#)
- [DCSync](#)
• Enumeration of Local Administrators
• GoldenTicket
• Kerberoasting
• Massive Computers Reconnaissance
• NTDS Extraction
• Password Guessing
• Password Spraying
• PetitPotam
• SAM Name Impersonation
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 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>
<th>Provider Name</th>
<th>Channel</th>
<th>Event IDs</th>
<th>Audit Policies</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other requirements</td>
<td>Handle Manipulation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sysmon extension</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Honey Account</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

See also

- [Credential Dumping: LSASS Memory](#)
- [DCShadow](#)
- [DCSync](#)
- [Domain Backup Key Extraction](#)
- [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</td>
<td>Success and Failure</td>
</tr>
<tr>
<td></td>
<td>⊲ — Sub-category: Kerberos Authentication Service</td>
<td></td>
</tr>
<tr>
<td>4769</td>
<td>⊲ Category: Account Logon</td>
<td>Success and Failure</td>
</tr>
<tr>
<td></td>
<td>⊲ — Sub-category: Kerberos Service Ticket Operations</td>
<td></td>
</tr>
<tr>
<td>4770</td>
<td>⊲ Category: Account Logon</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>⊲ — Sub-category: Kerberos Service Ticket Operations</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Requires Sysmon extension</strong></td>
<td>No</td>
</tr>
</tbody>
</table>

See also

- [Credential Dumping: LSASS Memory](#)
- [DCShadow](#)
- [DCSync](#)
- [Domain Backup Key Extraction](#)
- [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’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
- Domain Backup Key Extraction
- 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 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 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 only raises one alert with this IoA.

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

**Note:** Tenable.ad 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 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 NTLM: Audit Incoming NTLM Traffic</td>
<td>Enable auditing for all accounts</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>
<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: Logon</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Category: Account Logon</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sub-category: Kerberos Service Ticket Operations</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note: You can modify the options in bold.</td>
<td></td>
</tr>
</tbody>
</table>

### Other requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Requirement</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
• Domain Backup Key Extraction
• 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 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</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▼ Sub-category: Audit Application Generated</td>
<td></td>
</tr>
<tr>
<td>Microsoft-Windows-Security-Auditing</td>
<td>Security</td>
<td>4688</td>
<td>Category: Detailed Tracking</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▼ Sub-category: Audit Process Creation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▼ Sub-category:</td>
<td></td>
</tr>
<tr>
<td>Event Source</td>
<td>Category</td>
<td>Event ID</td>
<td>Event Details</td>
<td></td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-------------------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>ESENT</td>
<td>Application</td>
<td>325</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Microsoft-Windows-WMI-ACTIVITY</td>
<td>Security</td>
<td>4624</td>
<td>▼ Category: Logon/Logoff</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▼ Sub-category: Audit Logon</td>
<td></td>
</tr>
<tr>
<td>Microsoft-Windows-Security-Auditing</td>
<td>Security</td>
<td>4634</td>
<td>▼ Category: Logon/Logoff</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▼ Sub-category: Audit Logoff</td>
<td></td>
</tr>
<tr>
<td>Microsoft-Windows-Security-Auditing</td>
<td>Security</td>
<td>4689</td>
<td>▼ Category: Detailed Tracking</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▼ Sub-category: Audit Process Termination</td>
<td></td>
</tr>
<tr>
<td>Microsoft-Windows-Security-Auditing</td>
<td>Security</td>
<td>4674</td>
<td>▼ Category: Privilege Use</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▼ Sub-category: Audit Sensitive Privilege Use</td>
<td></td>
</tr>
</tbody>
</table>

Other requirements

- Sysmon extension: No
- Honey Account: No
See also

- [Credential Dumping: LSASS Memory](#)
- [DCShadow](#)
- [DCSync](#)
- [Domain Backup Key Extraction](#)
- [Enumeration of Local Administrators](#)
- [GoldenTicket](#)
- [Kerberosting](#)
- [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</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>Sub-category: Logon</td>
<td></td>
</tr>
<tr>
<td>4625</td>
<td>Category: Logon/Logoff</td>
<td>Failure</td>
</tr>
<tr>
<td></td>
<td>Sub-category: Logoff</td>
<td></td>
</tr>
<tr>
<td>4771</td>
<td>Category: Account Logon</td>
<td>Failure</td>
</tr>
<tr>
<td></td>
<td>Sub-category: Kerberos Authentication Serviced</td>
<td></td>
</tr>
<tr>
<td>4776</td>
<td>Category: Account Logon</td>
<td>Success and Failure</td>
</tr>
<tr>
<td></td>
<td>Sub-category: Credential Validation</td>
<td></td>
</tr>
</tbody>
</table>

Requires Sysmon extension No

See also

- [Credential Dumping: LSASS Memory](#)
- [DCShadow](#)
- [DCSync](#)
- [Domain Backup Key Extraction](#)
- [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>
<tbody>
<tr>
<td>4624</td>
<td>Category: Logon/Logoff</td>
<td></td>
</tr>
<tr>
<td></td>
<td>— Sub-category: Logon</td>
<td>Success</td>
</tr>
<tr>
<td>4625</td>
<td>Category: Logon/Logoff</td>
<td></td>
</tr>
<tr>
<td></td>
<td>— Sub-category: Logoff</td>
<td>Failure</td>
</tr>
<tr>
<td>4771</td>
<td>Category: Account Logon</td>
<td></td>
</tr>
<tr>
<td></td>
<td>— Sub-category: Kerberos Authentication Serviced</td>
<td>Failure</td>
</tr>
<tr>
<td>4776</td>
<td>Category: Account Logon</td>
<td></td>
</tr>
<tr>
<td></td>
<td>— 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](#)
- [Domain Backup Key Extraction](#)
- [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).

<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>--</td>
<td>Requires Sysmon extension</td>
<td>No</td>
</tr>
</tbody>
</table>

<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
• Domain Backup Key Extraction
• 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://github.com/rapid7/noPac)` and `[sam-the-admin](https://github.com/rapid7/sam-the-admin)`, as well as manual attacks using `[Rubeus](https://github.com/rapid7/rubeus)` and `[Impacket](https://github.com/rapid7/impacket)` 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 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 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>
</table>

Other requirements

- Sysmon extension: No
- Honey Account: No

See also

- [Credential Dumping: LSASS Memory](#)
- [DCShadow](#)
- [DCSync](#)
- [Domain Backup Key Extraction](#)
- [Enumeration of Local Administrators](#)
- [GoldenTicket](#)
- [Kerberasting](#)
- [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 requires Simple Mail Transfer Protocol (SMTP) configuration to send out alert notifications.

To configure the SMTP server:

1. In Tenable.ad, 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 to use when sending emails.
7. Click **Save**.

A message confirms that Tenable.ad updated the SMTP parameters.
Email Alerts

Tenable.ad 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:

![Email Alert Example](image)

To add an email alert:
1. In Tenable.ad, 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 sends out a notification on each deviant IoE detection.
   
   ○ **On each attack**: Tenable.ad 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 sends out a large volume of email notifications when a system reboot triggers alerts.
   
   ○ Unselect the checkbox: Tenable.ad 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 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 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 sent an email alert to the server.

11. Click **Add**.

    A message confirms that Tenable.ad created the email alert.

**To edit an email alert:**

1. In Tenable.ad, 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 updated the alert.

**To delete an email alert:**

1. In Tenable.ad, 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 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 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, 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 sends out a notification whenever an event that you specified occurs.
   - **On each deviance**: Tenable.ad sends out a notification on each deviant IoE detection.
   - **On each attack**: Tenable.ad 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 sends out a large volume of email notifications when a system reboot triggers alerts.

Unselect the checkbox: Tenable.ad 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 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 ✗ 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 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 sent a Syslog alert to the server.

11. Click **Add**.

   A message confirms that Tenable.ad created the Syslog alert.

To edit a Syslog alert:
1. In Tenable.ad, 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 updated the alert.

**To delete a Syslog alert:**

1. In Tenable.ad, 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 deleted the alert.

See also

- **Syslog and Email Alert Details**
Syslog and Email Alert Details

The following is an example of an alert:

Real-world example

```
<116>Jun 7 05:37:03 customer.tenable.ad TenableAD [1]: "0" "1" "FOREST" "DOMAIN" "C-PASSWORD-DONT-EXPIRE" "medium"
"CN=s_infosec.scanner,OU=ADManagers,DC=domain,DC=local" "24958" "1" "I-DONT-EXPIRE-SET" "40667" "Cn = s_infosec.scanner"

<113>Jun 8 05:37:03 customer.tenable.ad TenableAD [1]: "0" "1" "FOREST" "DOMAIN" "C-UNCONST-DELEG" "critical"
"CN=s_infosec.scanner,OU=ADManagers,DC=domain,DC=local" "38197" "1" "R-DELEG-PRIV USERS-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 deviance 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 deviance), &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_infosec.scanner,OU=ADManagers,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_infosec.scanner&quot;, &quot;CN=Backup Operators,CN=Builtin,DC=domain,DC=local&quot;</td>
</tr>
</tbody>
</table>
## EMAIL

<table>
<thead>
<tr>
<th>ID</th>
<th>Address</th>
<th>Severity threshold</th>
<th>Domains</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><a href="mailto:hello@tenable.com">hello@tenable.com</a></td>
<td>Medium</td>
<td>▲ 4 domains</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><a href="mailto:john.doe@tenable.com">john.doe@tenable.com</a></td>
<td>Medium</td>
<td>▲ 3 domains</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><a href="mailto:alan.smith@tenable.com">alan.smith@tenable.com</a></td>
<td>Medium</td>
<td>▲ 3 domains</td>
<td></td>
</tr>
</tbody>
</table>
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**.

![License Update Screen](image)

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**.

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

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