Decrypt domain traffic with a Windows domain controller

Published: 2025-01-24

The ExtraHop system can be configured to retrieve and store domain keys from one or more domain controllers. When the system observes encrypted traffic that matches the cached keys, all of the Kerberos-encrypted traffic in the domain is decrypted for supported protocols.

Active Directory is a frequent target for attackers because a successful attack campaign yields high-value targets. Critical attacks can be obscured by Kerberos or NTLM decryption, such as Golden Ticket, PrintNightmare, and Bloodhound. Decrypting this type of traffic can provide deeper insight for security detections.

You can enable decryption on an individual sensor or through an integration on RevealX 360. You can add more than one domain controller connection from a sensor to decrypt traffic from multiple domains.

The system only synchronizes Kerberos and NTLM decryption keys. Sensors operate in read-only mode and do not modify any properties in the domain. Decryption keys are cached in sensor memory and can not be removed from the sensor.

The following requirements must be met for decryption:

- You must have an Active Directory domain controller (DC) that is not configured as a Read-only Domain Controller (RODC).
- Only Windows Server 2016, Windows Server 2019, and Windows Server 2022 are supported.
- The ExtraHop system synchronizes keys for up to 50,000 accounts in a configured domain. If your DC has more than 50,000 accounts, some traffic will not be decrypted.
- The ExtraHop system must observe the network traffic between the DC and connected clients and servers.
- The ExtraHop system must be able to access the domain controller over the following ports: TCP 88 (Kerberos), TCP 445 (SMB), TCP 135 (RPC), and TCP ports 49152-65535 (RPC dynamic range).

> ⚠ **Warning:** If you enable these settings, the ExtraHop system is granted access to all of the account keys in the Windows domain. The ExtraHop system should be deployed at the same security level as the domain controller. Here are some best practices to consider:
>
> - Strictly limit end-user access to sensors that are configured with access to the domain controller. Ideally, only permit end-user access to a connected console.
> - Configure sensors with an identity provider that has strong authentication features such as two-factor or multi-factor authentication.
> - Restrict inbound and outbound traffic to and from the sensor to only what is needed.
> - In Active Directory, limit the Logon Workstations for the account to only communicate with the domain controller that the ExtraHop system is configured with.

Connect a domain controller to a sensor

Before you begin
You must have a user account with setup or system and access administration privileges on the sensor.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the System Configuration section, click **Capture**.
3. Click **Domain Controller**.
4. Click **Add Domain Controller Connection**.

5. Complete the following fields to specify credentials for the Microsoft Active Directory domain controller you want to connect to this sensor:

   • **Host:** The fully qualified domain name of the domain controller.

   • **Computer Name (sAMAccountName):** The name of the domain controller.

   • **Realm Name:** The name of the Kerberos realm where the domain controller has authority.

   • **Username:** The name of a user who is a member of the built-in Administrators group for the domain (not to be confused with the Domain Admins group). To prevent possible connection errors, specify a user account created after the domain controller was established.

   • **Password:** The password of the privileged user.
6. Click **Test Connection** to confirm that the sensor can communicate with the domain controller.
7. Click **Save**.
   The connection status and a timestamp of the last successful sync are displayed.

Next steps

- Click **Add Domain Controller Connection** to connect to another domain controller.
- Click **Change User Credentials** from a saved connection to modify credentials associated with the connection.
- Click **Remove Connection** to delete all credentials associated with the connection and disconnect the domain controller from the sensor.

Connect a domain controller to a RevealX 360 sensor

Before you begin
Your user account must have privileges on RevealX 360 for System and Access Administration.

1. Log into RevealX 360.
2. Click the System Settings icon ⚙ and then click **Integrations**.
3. Click the **Microsoft Protocol Decryption** tile.
4. Click **Add Credentials**.
5. Complete the following fields to specify credentials for the Microsoft Active Directory domain controller you want to connect to a RevealX 360 sensor:

   • **Host:** The fully qualified domain name of the domain controller.

   • **Computer Name (sAMAccountName):** The name of the domain controller.

   • **Realm Name:** The name of the Kerberos realm where the domain controller has authority.

   • **Username:** The name of a user who is a member of the built-in Administrators group for the domain (not to be confused with the Domain Admins group). To prevent possible connection errors, specify a user account created after the domain controller was established.

   • **Password:** The password of the privileged user.
6. From the drop-down menu, select the RevealX 360 sensor the domain controller will connect to.
7. Click **Test Connection** to confirm that the sensor can communicate with the domain controller.
8. Click **Connect**.
   The connection status and a timestamp of the last successful sync are displayed.

Next steps

- Click **Add Domain Controller Connection** to connect to another domain controller.
- Click **Change User Credentials** from a saved connection to modify credentials associated with the connection.
- Click **Delete Credentials** to delete all credentials associated with the connection and disconnect the domain controller from the sensor.

Validate the configuration settings

To validate that the ExtraHop system is able to decrypt traffic with configured domain controllers, go to the built-in Microsoft Protocol Decryption dashboard to identify successful decryption attempts.

Each chart in the Microsoft Protocol Decryption dashboard contains visualizations of Kerberos decryption data that have been generated over the selected time interval, organized by region.

The Microsoft Protocol Decryption dashboard is a built-in, system dashboard that you cannot edit, delete, or add to a shared collection. However, you can copy a chart from the Microsoft Protocol Decryption dashboard and add it to a custom dashboard, or you can make a copy of the dashboard and edit it to monitor metrics that are relevant to you.

Note: The Microsoft Protocol Decryption dashboard can only be viewed on a console.

The following information summarizes each region and its charts.

Kerberos Decryption Attempts

Observe the number of Kerberos decryption attempts in your environment in the following charts:

• **Successful Kerberos Decryption Attempts:** Total number of successful Kerberos decryption attempts and when they occurred.

• **Total Successful Attempts:** Total number of successful Kerberos decryption attempts.

• **Unsuccessful Kerberos Decryption Attempts:** Total number of unsuccessful Kerberos decryption attempts and when they occurred, listed by the reason the attempt failed.

• **Total Unsuccessful Attempts:** Total number of unsuccessful Kerberos decryption attempts, listed by the reason the attempt failed.

Unsuccessful Kerberos Decryption Details

Observe details about unsuccessful Kerberos decryption attempts in the following charts:

• **Unrecognized Server Principal Names:** Total number of Kerberos decryption attempts that failed due to an unrecognized server principal name (SPN), listed by the SPN. Displayed as a bar chart and a list chart.

• **Invalid Kerberos Keys:** Total number of Kerberos decryption attempts that failed due to an invalid Kerberos key, listed by the SPN that made the attempt. Displayed as a bar chart and a list chart.

• **Kerberos Decryption Errors :** Total number of Kerberos decryption attempts that failed due to an error, listed by the SPN that made the attempt. Displayed as a bar chart and a list chart.

Server Principal Name Details

Observe the top SPN that made Kerberos decryption attempts in the following charts:

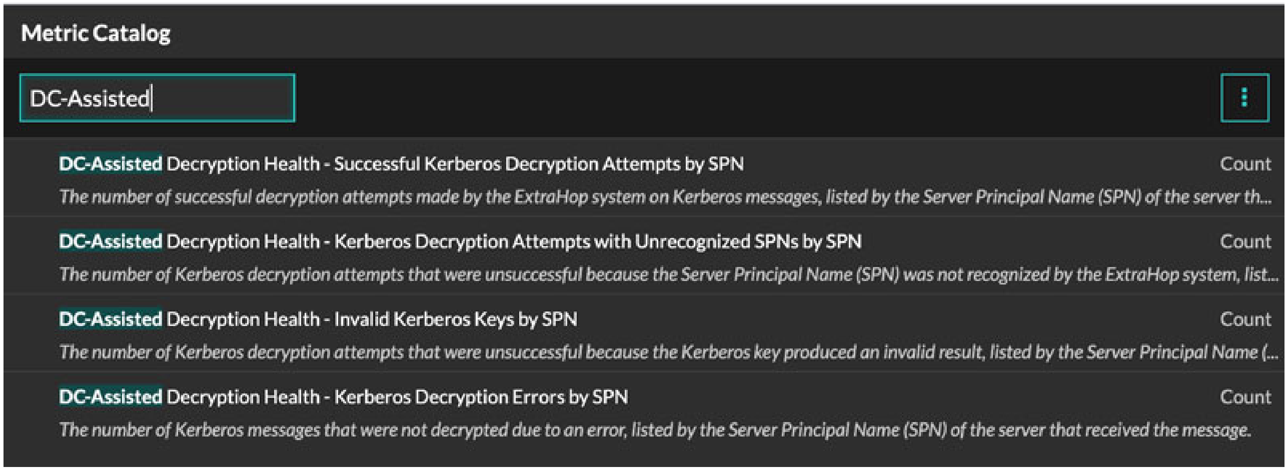
• **Top Server Principal Names:** Top 50 SPNs that made Kerberos decryption attempts and the following details:

- The number of successful decryption attempts.
- The number of unsuccessful attempts due to an invalid Kerberos key.
- The number of unsuccessful attempts due to an error.
- The number of unsuccessful attempts due an unrecognized SPN.

Additional system health metrics

The ExtraHop system provides metrics that you can add to a dashboard to monitor DC-assisted decryption health and functionality.

To view a list of available metrics, click the System Settings icon ⚙ and then click **Metric Catalog**. Type `DC-Assisted` in the filter field to display all available DC-assisted decryption metrics.



Metric Catalog

DC-Assisted

DC-Assisted Decryption Health - Successful Kerberos Decryption Attempts by SPN — Count

The number of successful decryption attempts made by the ExtraHop system on Kerberos messages, listed by the Server Principal Name (SPN) of the server th...

DC-Assisted Decryption Health - Kerberos Decryption Attempts with Unrecognized SPNs by SPN — Count

The number of Kerberos decryption attempts that were unsuccessful because the Server Principal Name (SPN) was not recognized by the ExtraHop system, list...

DC-Assisted Decryption Health - Invalid Kerberos Keys by SPN — Count

The number of Kerberos decryption attempts that were unsuccessful because the Kerberos key produced an invalid result, listed by the Server Principal Name (...

DC-Assisted Decryption Health - Kerberos Decryption Errors by SPN — Count

The number of Kerberos messages that were not decrypted due to an error, listed by the Server Principal Name (SPN) of the server that received the message.