

# Entschlüsseln Sie den Domänenverkehr mit einem Windows-Domänencontroller

Veröffentlicht: 2024-02-21


Das ExtraHop-System kann so konfiguriert werden, dass Domänenschlüssel von einem Domänencontroller abgerufen und gespeichert werden. Wenn das System verschlüsselten Verkehr beobachtet, der den gespeicherten Schlüsseln entspricht, wird der gesamte Kerberos-verschlüsselte Verkehr in der Domäne für unterstützte Protokolle entschlüsselt. Das System synchronisiert nur Kerberos- und NTLM-Entschlüsselungsschlüssel und ändert keine anderen Eigenschaften in der Domäne.

Ein Domänencontroller wie Active Directory ist ein häufiges Ziel von Angreifern, da eine erfolgreiche Angriffskampagne hochwertige Ziele hervorbringt. Kritische Angriffe wie Golden Ticket, PrintNightmare und Bloodhound können durch Kerberos- oder NTLM-Entschlüsselung verdeckt werden. Die Entschlüsselung dieser Art von Datenverkehr kann tiefere Einblicke in Sicherheitserkennungen liefern.

Sie können die Entschlüsselung für eine Person aktivieren Sensor oder durch eine Integration auf Reveal (x) 360.

Für die Entschlüsselung müssen die folgenden Anforderungen erfüllt sein:

- Sie müssen über einen Active Directory Directory-Domänencontroller (DC) verfügen, der nicht als schreibgeschützter Domänencontroller (RODC) konfiguriert ist.
- Nur Windows Server 2016 und Windows Server 2019 werden unterstützt.
- Nur ein Domänencontroller kann auf einem konfiguriert werden Sensor, was bedeutet, dass Sie den Traffic von einer Domain pro Domain entschlüsseln können Sensor.
- Das ExtraHop-System synchronisiert Schlüssel für bis zu 50.000 Konten in einer konfigurierten Domain. Wenn Ihr DC mehr als 50.000 Konten hat, wird ein Teil des Datenverkehrs nicht entschlüsselt.
- Das ExtraHop-System muss den Netzwerkverkehr zwischen dem DC und den angeschlossenen Clients und Servern beobachten.
- Das ExtraHop-System muss über die folgenden Ports auf den Domänencontroller zugreifen können: TCP 88 (Kerberos), TCP 445 (SMB), TCP 135 (RPC) und TCP-Ports 49152-65535 (RPC-Dynamikbereich).

 **Warnung:** Wenn Sie diese Einstellungen aktivieren, erhält das ExtraHop-System Zugriff auf alle Kontoschlüssel in der Windows-Domäne. Das ExtraHop-System sollte auf derselben Sicherheitsstufe wie der Domänencontroller bereitgestellt werden. Hier sind einige bewährte Methoden, die Sie berücksichtigen sollten:

- Beschränken Sie den Endbenutzerzugriff strikt auf Sensoren die mit Zugriff auf den Domänencontroller konfiguriert sind. Erlauben Sie im Idealfall nur Endbenutzern den Zugriff auf ein verbundenes Konsole.
- Konfigurieren Sie Sensoren mit einem Identitätsanbieter, der über starke Authentifizierungsfunktionen wie Zweifaktor- oder Multi-Faktor-Authentifizierung verfügt.
- Beschränken Sie den eingehenden und ausgehenden Verkehr zum und vom Sensor nur auf das, was benötigt wird.
- Beschränken Sie in Active Directory die Logon-Workstations für das Konto so, dass sie nur mit dem Domänencontroller kommunizieren, mit dem das ExtraHop-System konfiguriert ist.

## Einen Domänencontroller mit einem Sensor verbinden

### Bevor Sie beginnen


Sie benötigen ein Benutzerkonto mit Setup oder [System- und Zugriffsadministrationsrechte](#) auf dem Sensor.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Erfassung**.
3. klicken **Domänencontroller**.
4. Wählen Sie den **Verbindung zum Domänencontroller aktivieren** Checkbox.
5. Füllen Sie die folgenden Felder aus:
  - **Hostname:** Der vollqualifizierte Domänenname des Domänencontroller.
  - **Computername (sAMAccountName):** Der Name des Domänencontroller.
  - **Name des Bereichs:** Der Kerberos-Bereichsname des Domänencontroller.
  - **Nutzername:** Der Name eines Benutzers, der Mitglied der integrierten Administratorgruppe für die Domain ist (nicht zu verwechseln mit der Gruppe Domain-Admins). Um mögliche Verbindungsfehler zu vermeiden, geben Sie ein Benutzerkonto an, das nach der Einrichtung des Domänencontrollers erstellt wurde.
  - **Passwort:** Das Passwort des privilegierten Benutzers.
6. klicken **Verbindung testen** um zu bestätigen, dass der Sensor mit dem Domänencontroller kommunizieren kann.
7. klicken **Speichern**.

## Einen Domänencontroller mit einem Reveal (x) 360-Sensor verbinden

### Bevor Sie beginnen

Ihr Benutzerkonto muss [Privilegien](#) auf Reveal (x) 360 für System - und Zugriffsadministration.

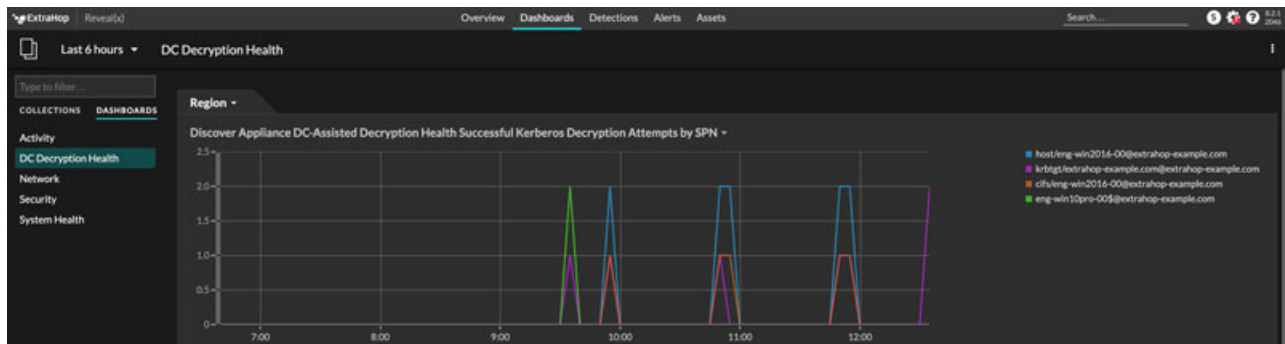
1. Loggen Sie sich bei Reveal (x) 360 ein.
2. Klicken Sie auf das Symbol Systemeinstellungen  und dann klicken **Integrationen**.
3. Klicken Sie auf **Microsoft-Protokollentschlüsselung** Kachel.
4. Füllen Sie die folgenden Felder aus, um Anmeldedaten für den Microsoft Active Directory-Domänencontroller anzugeben, den Sie mit einem Reveal (x) 360-Sensor verbinden möchten:
  - **Hostname:** Der vollqualifizierte Domänenname des Domänencontroller.
  - **Computername (sAMAccountName):** Der Name des Domänencontroller.
  - **Name des Bereichs:** Der Kerberos-Bereichsname des Domänencontroller.
  - **Nutzername:** Der Name eines Benutzers, der Mitglied der integrierten Administratorgruppe für die Domain ist (nicht zu verwechseln mit der Gruppe Domain-Admins). Um mögliche Verbindungsfehler zu vermeiden, geben Sie ein Benutzerkonto an, das nach der Einrichtung des Domänencontrollers erstellt wurde.
  - **Passwort:** Das Passwort des privilegierten Benutzers.
5. Wählen Sie aus der Dropdownliste den Reveal (x) 360-Sensor aus, mit dem der Domänencontroller eine Verbindung herstellen soll. Nur ein Domänencontroller kann an einen Reveal (x) 360-Sensor angeschlossen werden.
6. klicken **Verbindung testen** um zu bestätigen, dass der Sensor mit dem Domänencontroller kommunizieren kann.
7. klicken **Speichern**.

## Überprüfen Sie die Konfigurationseinstellungen

Um zu überprüfen, ob das ExtraHop-System den Datenverkehr mit dem Domänencontroller entschlüsseln kann, erstellen Sie ein Dashboard, das erfolgreiche Entschlüsselungsversuche identifiziert.

1. [Neues Dashboard erstellen](#)
2. Klicken Sie auf das Diagramm-Widget, um die Metrikquelle hinzuzufügen.
3. klicken **Quelle hinzufügen**.
4. Geben Sie im Feld Quellen den Namen der Sensor Kommunizieren Sie mit einem Domänencontroller und wählen Sie dann Sensor aus der Liste.
5. Geben Sie im Feld Metriken Folgendes ein: DC im Suchfeld und dann wählen **Integrität der DC-gestützten Entschlüsselung – Erfolgreiche Kerberos-Entschlüsselungsversuche von SPN**.
6. klicken **Speichern**.

Das Diagramm wird mit der Anzahl der erfolgreichen Entschlüsselungsversuche angezeigt.



## Zusätzliche Metriken zur Systemintegrität

Das ExtraHop-System bietet Metriken, die Sie einem Dashboard hinzufügen können, um den Zustand und die Funktionalität der DC-gestützten Entschlüsselung zu überwachen.

Um eine Liste der verfügbaren Messwerte anzuzeigen, klicken Sie auf das Symbol Systemeinstellungen und dann klicken **Metrischer Katalog**. Typ DC-unterstützt im Filterfeld, um alle verfügbaren Metriken zur DC-unterstützten Entschlüsselung anzuzeigen.

Metric Catalog	
DC-Assisted	
<b>DC-Assisted</b> Decryption Health - Successful Kerberos Decryption Attempts by SPN	Count
<i>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...</i>	
<b>DC-Assisted</b> Decryption Health - Kerberos Decryption Attempts with Unrecognized SPNs by SPN	Count
<i>The number of Kerberos decryption attempts that were unsuccessful because the Server Principal Name (SPN) was not recognized by the ExtraHop system, list...</i>	
<b>DC-Assisted</b> Decryption Health - Invalid Kerberos Keys by SPN	Count
<i>The number of Kerberos decryption attempts that were unsuccessful because the Kerberos key produced an invalid result, listed by the Server Principal Name (...)</i>	
<b>DC-Assisted</b> Decryption Health - Kerberos Decryption Errors by SPN	Count
<i>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.</i>	