

IBM QRadar User Entity Behavior Analytics
app
5.0.1

User Guide



Note

Before you use this information and the product that it supports, read the information in [“Notices” on page 287](#).

Contents

- Chapter 1. QRadar User Entity Behavior Analytics.....1**
 - What's new in the QRadar User Entity Behavior Analytics app..... 2
 - Earlier versions..... 11
 - Known issues..... 12
 - Process overview..... 13
 - Entity overview..... 14
 - UEBA overview and user details..... 17
 - Managing the UEBA dashboard views..... 22
 - Investigating users in QRadar Advisor with Watson..... 23
 - Prerequisites for installing the User Entity Behavior Analytics app..... 23
 - Log source types relevant to the UEBA app..... 24
 - Deleting users or entities from UEBA..... 24

- Chapter 2. Installing and uninstalling..... 25**
 - Installing the User Entity Behavior Analytics app..... 25
 - Uninstalling the UEBA app..... 26

- Chapter 3. Upgrading the UEBA app..... 29**

- Chapter 4. Configuring the User Entity Behavior Analytics app..... 31**
 - Configuring UEBA settings..... 31
 - Configuring the authorization token in QRadar settings..... 31
 - Configuring content package settings..... 32
 - Configuring application settings..... 32
 - Configure user import..... 35
 - Importing users..... 35
 - Importing users with LDAP or Active Directory..... 37
 - Importing users from a reference table..... 38
 - Importing users from a CSV file..... 40
 - Tuning user import configurations..... 41
 - How user imports in UEBA synchronizes imported data to a reference table..... 44

- Chapter 5. Administering..... 47**
 - Administrative functions..... 47
 - Assigning user capabilities for the QRadar User Entity Behavior Analytics app..... 47
 - Creating watchlists..... 48
 - Viewing the trusted users list..... 52
 - Managing network monitoring tools..... 53
 - Managing restricted programs..... 53
 - Adding log sources to the trusted log source group..... 54
 - New accounts..... 54
 - Dormant accounts..... 55
 - Resetting machine learning model..... 56
 - Active investigation in User Entity Behavior Analytics app..... 57

- Chapter 6. Tuning..... 61**
 - Enabling indexes to improve performance..... 61
 - Integrating new or existing QRadar content with the UEBA app..... 62
 - Integrating content without QRadar Use Case Manager (or QRadar Use Case Manager 3.1.0 or earlier)..... 63

Integrating content with Use Case Manager 3.2.0 or later.....	63
Tuning entity assets.....	64
UEBA common challenges.....	64
Reference sets.....	69
Chapter 7. Multitenancy in UEBA.....	71
QRadar configurations for setting up multitenancy in UEBA.....	73
Installing and configuring UEBA instances to support multitenancy.....	76
Installing and configuring Machine Learning in Multitenancy.....	77
UEBA user roles for multitenancy.....	78
Rules and tuning for multitenancy in UEBA.....	80
Chapter 8. Rules and tuning for the UEBA app.....	83
UEBA content pack summary.....	83
UEBA 5.x rules.....	84
Access and authentication.....	86
UEBA : Bruteforce Authentication Attempts.....	86
UEBA : Detected Activity from a Locked Machine.....	87
UEBA : Executive only asset accessed by non-executive user from external network.....	88
UEBA : Executive only asset accessed by non-executive user from internal network.....	88
UEBA : High Risk User Access to Critical Asset.....	89
UEBA : Large number of denied access events towards external domain.....	91
UEBA : Multiple VPN Accounts Failed Login From Single IP.....	91
UEBA : Multiple VPN Accounts Logged In From Single IP.....	92
UEBA : Remote access hole in corporate firewall.....	93
UEBA : Repeat Unauthorized Access.....	94
UBA : Terminated User Activity.....	95
UBA : Unauthorized Access.....	95
UEBA : Unix/Linux System Accessed With Service or Machine Account.....	97
UEBA : User Access - Failed Access to Critical Assets.....	97
UEBA : First Access to Critical Assets.....	99
UBA : User Access from Multiple Hosts.....	101
UEBA : User Access to Internal Server From Jump Server	102
UBA : Login Anomaly.....	104
UEBA : User Accessing Account from Anonymous Source.....	104
UEBA : User Access at Unusual Times.....	106
UBA : VPN Access By Service or Machine Account.....	107
UBA : VPN Certificate Sharing.....	108
UBA : Windows Access with Service or Machine Account.....	109
Accounts and privileges.....	109
UBA : Account or Group or Privileges Added.....	109
UEBA : Account or Group or Privileges Modified.....	111
UBA : DoS Attack by Account Deletion.....	113
UEBA : User Account Created and Deleted in a Short Period of Time.....	116
UEBA : Dormant Account Used.....	118
UEBA : Dormant Account Use Attempted.....	119
UEBA : Expired Account Used.....	121
UEBA : First Privilege Escalation.....	123
UBA : New Account Use Detected.....	125
UEBA : Suspicious Privileged Activity (First Observed Privilege Use).....	126
UEBA : Suspicious Privileged Activity (Rarely Used Privilege).....	128
UEBA : User Attempt to Use Disabled Account.....	131
UEBA : User Attempt to Use a Suspended Account.....	132
Browsing behavior.....	134
UBA : Browsed to Business/Service Website.....	134
UBA : Browsed to Communications Website.....	135
UBA : Browsed to Education Website.....	137

UBA : Browsed to Entertainment Website.....	138
UEBA : Browsed to Gambling Website.....	140
UBA : Browsed to Government Website.....	142
UBA : Browsed to Information Technology Website.....	143
UBA : Browsed to Job Search Website.....	145
UEBA : Browsed to LifeStyle Website.....	146
UBA : Browsed to Malicious Website.....	148
UBA : Browsed to Mixed Content/Potentially Adult Website.....	149
UBA : Browsed to Phishing Website.....	151
UEBA : Browsed to Pornography Website.....	152
UBA : Browsed to Religious Website.....	154
UBA : Browsed to Scam/Questionable/Illegal Website.....	156
UBA : Browsed to Social Networking Website.....	157
UEBA : Browsed to Uncategorized Website.....	159
UBA: User Accessing Risky URL.....	160
Cloud.....	162
UEBA : Anonymous User Accessed a Resource.....	162
UBA : AWS Console Accessed by Unauthorized User.....	162
UBA : External User Failed Mailbox Login.....	163
UBA : Failed to Set Mailbox Audit Logging Bypass.....	164
UEBA : Inbox Set to Forward to External Inbox.....	164
UBA : Internal User Failed Mailbox Login Followed by Success.....	165
UBA : Mailbox Permission Added and Deleted in a Short Period of Time.....	165
UBA : Non-Standard User Accessing AWS Resources.....	166
UBA : Sharing Link Sent to Guest.....	166
UBA : Sharing Policy Changed or Shared External (SharePoint/OneDrive).....	167
UBA : User Added to a Group on SharePoint or OneDrive by Site Admin.....	167
UBA : User Failed to be Added to Role.....	167
Domain controller.....	168
UBA : DPAPI Backup Master Key Recovery Attempted.....	168
UEBA : Kerberos Account Enumeration Detected.....	168
UBA : Multiple Kerberos Authentication Failures from Same User.....	169
UBA : Non-Admin Access to Domain Controller.....	170
UBA : Pass the Hash.....	171
UBA : Possible Directory Services Enumeration.....	172
UBA : Possible SMB Session Enumeration on a Domain Controller.....	172
UBA : Possible TGT Forgery.....	173
UBA : Possible TGT PAC Forgery.....	173
UBA : Replication Request from a Non-Domain Controller.....	174
UEBA : TGT Ticket Used by Multiple Hosts.....	174
Endpoint.....	175
UEBA : Detect Insecure Or Non-Standard Protocol.....	175
UEBA : Detect Persistent SSH session.....	176
UBA : Internet Settings Modified.....	179
UBA : Malware Activity - Registry Modified In Bulk.....	180
UBA : Netcat Process Detection (Linux).....	181
UBA : Netcat Process Detection (Windows).....	182
UBA : Process Executed Outside Gold Disk Allowlist (Linux).....	183
UBA : Process Executed Outside Gold Disk Allowlist (Windows).....	185
UEBA : Ransomware Behavior Detected.....	186
UEBA : Restricted Program Usage.....	187
UBA : User Installing Suspicious Application.....	189
UBA : Volume Shadow Copy Created.....	190
Exfiltration.....	191
UEBA : Data Exfiltration by Cloud Services.....	191
UEBA : Data Exfiltration by Print.....	192
UEBA : Data Exfiltration by Removable Media.....	192
UEBA : Data Loss Possible.....	193

UEBA : Initial Access Followed by Suspicious Activity.....	194
UEBA : Large Outbound Transfer by High Risk User.....	195
UEBA : Multiple Blocked File Transfers Followed by a File Transfer.....	196
UEBA : Multiple blocked file uploads followed by a successful upload.....	198
UEBA : Potentially Compromised Account.....	198
UEBA : Suspicious Access Followed by Data Exfiltration.....	199
UEBA : Suspicious Activity Followed by Exfiltration.....	200
UEBA : User Potentially Phished.....	201
Geography.....	202
UBA : Anomalous Account Created From New Location.....	202
UBA : Anomalous Cloud Account Created From New Location.....	205
UBA : User Access from Multiple Locations.....	206
UEBA : User Access from Prohibited Location.....	208
UEBA : User Access from Restricted Location.....	210
UEBA : User Geography Change.....	212
UBA : User Access from Unusual Locations.....	214
MaaS360 Security.....	216
UBA : MaaS360 detected device with low encryption level.....	216
UBA : MaaS360 device out of compliance due to non-roaming data usage.....	216
UBA : MaaS360 device out of compliance due to device being rooted.....	217
UBA : MaaS360 device out of compliance due to encryption level.....	217
UBA : MaaS360 device out of compliance due to OS version.....	218
UBA : MaaS360 malicious SMS received.....	218
UBA : MaaS360 malicious email received.....	219
UBA : MaaS360 URL access blocked.....	219
UBA : MaaS360 malware application installed.....	220
UBA : MaaS360 malicious URL accessed.....	220
Network traffic and attacks.....	221
UEBA : D/DoS Attack Detected.....	221
UEBA : Honeytoken Activity.....	222
UBA : Network Traffic : Capture Monitoring and Analysis Program Usage.....	223
QRadar DNS Analyzer.....	225
UBA : Potential Access to Blocklist Domain.....	225
UBA : Potential Access to DGA Domain.....	225
UBA : Potential Access to Squatting Domain.....	226
UBA : Potential Access to Tunneling Domain.....	226
Threat intelligence.....	227
UBA : Detect IOCs For Locky.....	227
UEBA : Detect IOCs for WannaCry.....	228
UBA : Multiple Sessions to Monitored Log Sources (NIS Directive).....	228
UBA : ShellBags Modified By Ransomware.....	229
UEBA : User Accessing Risky IP Anonymization.....	229
UBA : User Accessing Risky IP Botnet.....	230
UEBA : User Accessing Risky IP Dynamic.....	231
UEBA : User Accessing Risky IP Malware.....	231
UEBA : User Accessing Risky IP Spam.....	232
Supported QRadar content.....	232
Changed implementation for rules.....	235

Chapter 9. Machine Learning Analytics app.....	239
Known issues for Machine Learning Analytics.....	239
Prerequisites for installing the Machine Learning Analytics app.....	239
Installing the Machine Learning Analytics app.....	240
UEBA dashboard with Machine Learning.....	241
Uninstalling the Machine Learning Analytics app.....	246

Chapter 10. Machine Learning user models.....	247
--	------------

Individual (Numeric) user models.....	248
Access activity.....	248
Aggregated Activity.....	250
Authentication Activity.....	250
Data Downloaded.....	251
Data Uploaded to Remote Networks.....	252
DDL events.....	252
DML events.....	253
HTTP Data Transfer Activity.....	253
Outbound Transfer Attempts.....	254
Risk Posture.....	254
Successful Access and Authentication Activity.....	254
Suspicious Activity.....	255
Individual (Observable) user models	256
Lateral Movement : Internal Asset Usage.....	256
Lateral Movement : Internal Destination Port Activity.....	257
Lateral Movement : Network Zone Activity.....	258
Process Usage.....	258
Peer group models.....	259
Activity Distribution.....	259
Defined Peer Group.....	260
Internal Asset Access by Peer Group.....	260
Internal Destination Ports by Peer Group.....	261
Learned Peer Group.....	261
Network Zones by Peer Group.....	262
Process Execution by Peer Group.....	262
<i>Creating a custom model.....</i>	263
Application Events.....	267
Destination Port.....	268
Office File Access.....	268
AWS Access.....	268
Process.....	268
Website.....	268
Risky IP.....	269
Peer group model grouping requirements.....	269
Machine learning analytic requirements.....	270
Chapter 11. Troubleshooting and support.....	273
Help and support page for UEBA.....	273
Service requests.....	274
Machine Learning supervisorctl status shows EXITED.....	274
Machine Learning app status shows warning on dashboard.....	274
Machine Learning status shows no progress for data ingestion.....	274
ML app status is in an error state.....	275
Downloading UEBA and Machine Learning logs.....	276
Chapter 12. APIs for UEBA.....	277
Public API documentation for UEBA.....	277
User above threshold.....	277
User information.....	278
Investigated users.....	278
Top 10 risky users.....	279
Top 10 anomalous users.....	279
Single user information.....	280
User risk score information.....	280
UEBA generated offenses.....	280
User import.....	281

Notices.....	287
Trademarks.....	288
Terms and conditions for product documentation.....	288
IBM Online Privacy Statement.....	289
General Data Protection Regulation.....	289

Chapter 1. QRadar User Entity Behavior Analytics

The IBM® QRadar® User Entity Behavior Analytics app helps you to determine the risk profiles of users and entity inside your network and to take action when the app alerts you to threatening behavior.

The QRadar User Entity Behavior Analytics (UEBA) app is a tool for detecting insider threats in your organization. It is built on top of the app framework to use existing data in your QRadar to generate new insights around users and entity risk. UEBA adds two major functions to QRadar: risk of user and entity, and unified user identities.

Risk profiling is done by assigning risk to different security use cases. Examples might include simple rules and checks such as bad websites, or more advanced stateful analytics that use machine learning. Risk is assigned to each one depending on the severity and reliability of the incident detected. UEBA uses existing event and flow data in your QRadar system to generate these insights and profile risks of users.

UEBA uses three types of traffic that enrich UEBA and enable more use cases to profile risk. The three types are as follows:

1. Traffic around access, authentication, and account changes.
2. User behavior on the network, so devices such as: proxies, firewalls, IPS, and VPNs.
3. Endpoint and application logs, such as from Windows or Linux®, and SaaS applications.

Unifying user identities is accomplished by combining disparate accounts for a user in QRadar. By importing data from an Active Directory, an LDAP server, Reference table, or CSV file, UEBA can be taught what accounts belong to a user identity. This helps combine risk and traffic across the different user names in UEBA.

Machine Learning (ML app) is an add-on tool that augments the UEBA app. It enables more rich and in-depth use cases that perform time series profiling and clustering. It is installed from within the UEBA app, on the Machine Learning settings page. The ML app adds visualizations to the existing UEBA app that show learned behavior (models), current behavior, and alerts. The models can use more than four weeks of historical data in QRadar to make the predictive models and baselines of what is normal for a user.

For more information about using the ML app, see [Chapter 9, “Machine Learning Analytics app,” on page 239](#).

Importing users and user data

You can import users and user data with the User import wizard. The User import wizard helps you to import users from an LDAP server, an Active Directory server, from reference tables, and CSV files. You can also create custom attributes with the User import wizard

For more information about importing user data with the User import wizard, see [“Configure user import” on page 35](#).

Rules and tuning

Consider the following important information about rules and tuning in UEBA.

- UEBA rule content is installed after the app is configured.
- Rules should be edited in the QRadar Use Case Manager app
- The rules that will produce a risk score for users are added to the UBA : Rule Data table. Building blocks and rules that do not produce risk score are not added.
- A poll task runs that adds new rules created by users that contain '*senseValue=#*' in the event description.
- Existing rules should not be edited. You should make copies and ensure the *eventname* is also changed.

For more information, see [Chapter 8, “Rules and tuning for the UEBA app,” on page 83](#).

Browser conformance

UEBA is supported on Google Chrome and Mozilla Firefox.

Note: To maximize your experience with UEBA, you should do one of the following:

- Disable the pop-up blocker for your browser
- Configure your browser to allow exceptions for pop-ups coming from the QRadar Console IP address

Related concepts

[“Rules and tuning for the UEBA app” on page 83](#)

The IBM QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[“Configuring the User Entity Behavior Analytics app” on page 31](#)

Before you can use the IBM QRadar User Entity Behavior Analytics (UEBA) app, you must configure additional settings.

[“Machine Learning Analytics app” on page 239](#)

The Machine Learning Analytics (ML) app extends the capabilities of your QRadar system and the QRadar User Entity Behavior Analytics (UEBA) app by adding use cases for machine learning analytics. With the machine learning analytics models, you can gain additional insight into user behavior with predictive modeling. The ML app helps your system to learn the expected behavior of the users in your network.

Related tasks

[“Installing the User Entity Behavior Analytics app” on page 25](#)

Use the IBM QRadar Extension Management tool to upload and install your app archive directly to your QRadar Console.

[“Upgrading the UEBA app” on page 29](#)

To take advantage of new capabilities, defect fixes, and updated workflows, upgrade to new versions of QRadar User Entity Behavior Analytics (UEBA). Use the Extensions Management tool in IBM QRadar to upgrade your app, or use the IBM QRadar Hub app to upgrade. You must be an administrator to upgrade to new versions of the app.

What's new in the QRadar User Entity Behavior Analytics app

Learn about the new features and enhancements in the latest QRadar User Entity Behavior Analytics (UEBA) app releases.

What's new in 5.1.0 (Released January 2026)



Attention: You must first upgrade to version 5.0.1 or later before upgrading the app to version 5.1.0.

- Updated 32 UEBA rules and added entity-level support.
- Added the ability to create entity-based and hybrid watchlist.
- Introduced active investigation functionality for entities.
- Enabled dark theme support for the following UEBA pages:
 - User Import
 - Rules
 - Machine learning
 - Setting
- Added support to reset individual ML models directly from the dashboard.
- Introduced the ability to delete entities and stop entity tracking.
- Improved performance for right-panel loading and details pages.
- Increased the default UEBA memory allocation from 1 GB to 1.1 GB.

- Resolved identified security vulnerabilities.
- Fixed multiple bug issues.

What's new in 5.0.3 (Released December 2025)

- Fixed critical Next.js vulnerability (CVE-2025-55182).

What's new in 5.0.2 (Released October 2025)

- Updated Spark to version 4.0.1 to fix several vulnerabilities.
- Upgraded Next.js to version 15.5.3 to address a vulnerability.
- Resolved a few additional vulnerabilities.
- Fixed a few bugs.

What's new in 5.0.1 (Released August 2025)

Upgrade note: You should upgrade to QRadar User Entity Behavior Analytics 4.1.17 before you upgrade to QRadar User Entity Behavior Analytics 5.0.1.

- User Behavior Analytics (UBA) is rebranded to User Entity Behavior Analytics (UEBA).
- Incorporated entity context, including device IP addresses, hostnames, and MAC addresses, along with risk profiling for entities.
- The UEBA dashboard now has a new "Entity Monitoring" widget, displaying the entity risk score.
- Added an Entity Details page that provides additional information about the specific entity, such as IP address, hostname, MAC address, geolocation, user sessions, and device vulnerability score.
- Added Entity Timeline that shows users, source IP addresses, and destination IP addresses, as well as source MAC addresses.
- UEBA now allows for the creation of entity-specific offenses.
- The UEBA settings page now shows new Entity Risk Threshold and Disable Entity Monitoring options.
- The search bar in the dashboard can now be used to search for both users and entities.
- Updated UEBA rules.

What's new in 4.1.17 (Released November 2024)

Upgrade note: You should upgrade to QRadar User Entity Behavior Analytics 4.1.10 before you upgrade to QRadar User Entity Behavior Analytics 4.1.17.

- Added the ability to show user import source in the User list and the **User details** page.
- Added the ability to allow users to edit the use case names in the user timeline.
- Added the ability to allow non-admin users to edit the watchlist.
- Fixed the duplicate database migration issue.
- Fixed a peer group model build issue in multitenant environments.
- Fixed security vulnerabilities.

What's new in 4.1.16 (Released May 2024)

- Added RBAC feature with two new roles: **Admin** and **Read-only user**. Admins can run all the operations in UEBA. Read-only users can only view information in UEBA.
- Java is now upgrade to version 17.
- Migrated to base image v3 in preparation to move to python 3.8.
- Fixed security vulnerabilities. For more information, see the following security bulletin: [CVE-2023-41419, CVE-2023-26159, CVE-2024-29180, CVE-2023-31486, CVE-2023-44981,](#)

CVE-2023-26145, CVE-2022-46751, CVE-2023-25613, CVE-2024-22195, CVE-2023-34453, CVE-2023-34454, CVE-2023-34455, CVE-2020-13936, CVE-2023-6378, CVE-2022-25647, CVE-2023-34462, CVE-2023-6481, CVE-2024-28849, CVE-2017-16137, CVE-2023-46234, CVE-2023-22946, CVE-2018-17190, CVE-2018-11804, CVE-2018-11770, CVE-2023-3635.

What's new in 4.1.15 (Released March 2024)

- Fixed an issue so that the app works with QRadar 7.5.0 Update Package 8.

What's new in 4.1.14 (Released November 2023)

- Improved UEBA to use correct IP address when encrypted App Host is used in NAT environment
- Enhanced Machine Learning to use correct IP address when the encrypted App Host is used in NAT environment.
- Machine Learning model now recovers itself when model build fails with the "lost user Id lookup object" error.
- Added the ability to gather additional files when using Machine Learning download logs function on the Help and Support page.
- Fixed an issue that caused an unexpected error when viewing user details in the QRadar Suite SOAR App.
- Fixed an issue that caused querying on custom machine learning model to fail validation when using with the character sequence '\$'.
- Fixed an issue that caused UBAController process to fail when saving a configuration that already existed in zookeeper.
- You can now select and delete multiple users at once on the Search Results page.
- You can now see the tenant name in the UBA Overview page header when using multitenant configuration.



What's new in 4.1.13 (Released August 2023)

- Added the ability to disable risk score decay by setting the "Decay risk by this factor per hour" option to "0" on the application settings page. For more information, see ["Configuring application settings" on page 32.](#)
- Error messages that relate to installing or uninstalling Machine Learning are now displayed for 30 seconds on the installer page.
- Fixed an issue that prevented proper redirection to QRadar Use Case Manager when you view a tenant instance of QRadar User Entity Behavior Analytics while you're logged in as an administrator.
- Fixed an issue where using the 'View User Details' link from QRadar to QRadar User Entity Behavior Analytics caused the wildcard search to use 'NULL' as the username and incorrectly match users to the original QRadar log activity or offenses record.
- Fixed an issue that prevented failed Machine Learning models to self-correct after receiving corrupted data.
- Fixed security vulnerabilities. For more information, see the following security bulletin: [CVE-2023-32697, CVE-2021-3803, CVE-2022-25883, CVE-2020-28498, CVE-2022-3517, CVE-2023-34104, CVE-2023-26920, CVE-2022-25858, CVE-2022-38900, CVE-2021-43803, CVE-2021-37699, CVE-2022-46175, CVE-2023-37920, CVE-2021-23440.](#)

What's new in 4.1.12 (Released June 2023)

- Enhanced the machine learning installation process to allow for different size installations on QRadar 7.5.0 in multitenant deployments. For more information, see [“Installing and configuring Machine Learning in Multitenancy” on page 77](#).
- Fixed an issue with viewing events from the graph of Machine Learning models "Data uploaded to remote networks and Data downloaded".
- Fixed an issue where the custom event property "UploadRatio" was undefined in QRadar 7.5.0.
- Adjusted right-click action on "View user details" to perform case-insensitive match for username.
- Fixed security vulnerabilities. For more information, see the following security bulletin: [CVE-2022-3171](#), [CVE-2022-41881](#), [CVE-2022-40152](#), [CVE-2022-31160](#), [CVE-2017-7525](#), [CVE-2022-25168](#), [CVE-2022-3509](#), [CVE-2022-41854](#), [CVE-2022-38752](#), [CVE-2022-1471](#), [CVE-2021-37533](#), [CVE-2022-42004](#), [CVE-2022-42003](#)

What's new in 4.1.11 (Released March 2023)

- Fixed an issue that caused TLS connection failures when using secure LDAP.
- Fixed security vulnerabilities. For more information, see the following security bulletin: [CVE-2019-6283](#), [CVE-2018-20821](#), [CVE-2018-11698](#), [CVE-2020-24025](#), [CVE-2018-19838](#), [CVE-2018-11694](#), [CVE-2018-19827](#), [CVE-2018-20190](#), [CVE-2019-6286](#), [CVE-2019-6284](#), [CVE-2018-19839](#), [CVE-2018-19797](#), [CVE-2022-37601](#), [CVE-2022-37603](#), [CVE-2022-37598](#), [CVE-2021-42581](#), [CVE-2021-39227](#), [CVE-2021-3765](#), [CVE-2022-31129](#), [CVE-2022-24785](#), [CVE-2021-23343](#), [CVE-2020-15366](#), [CVE-2021-23382](#), [CVE-2022-25927](#), [CVE-2022-37599](#), [CVE-2022-24999](#), [CVE-2021-32803](#), [CVE-2021-37712](#), [CVE-2021-37701](#), [CVE-2021-37713](#), [CVE-2021-32804](#), [CVE-2020-7764](#), [CVE-2021-23364](#), [CVE-2022-25758](#), [CVE-2021-23362](#), [CVE-2021-23368](#), [CVE-2021-3918](#), [CVE-2021-29060](#), [CVE-2022-25901](#), [CVE-2021-42740](#), [CVE-2021-3807](#)

What's new in 4.1.10 (Released February 2023)

- Upgraded the LDAPv3 Python library to address parsing issue in UEBA.
- Upgraded jQuery UI to address a vulnerability in UEBA.
- Updated user imports to fix an issue that caused automatic reruns.
- Increased the character limit for the LDAP filter to 1000.
- Updated Machine Learning to fix an issue that caused models to be stuck in the building phase.
- Fixed a security vulnerability. For more information, see the following security bulletin: [CVE-2022-23491](#)

What's new in 4.1.9 (Released September 2022)

- Updates to Ariel Query Language (AQL) to use new recommended constructs.
- Fixed security vulnerabilities. For more information, see the following security bulletins:
 - [CVE-2012-5783](#), [CVE-2021-22569](#), [CVE-2019-10202](#), [CVE-2019-10172](#), [CVE-2011-4969](#), [CVE-2015-9251](#), [CVE-2012-6708](#), [CVE-2020-7656](#), [CVE-2021-29425](#), [CVE-2020-9492](#), [CVE-2021-34538](#), [CVE-2019-0205](#), [CVE-2022-25647](#), [CVE-2020-13936](#)
 - [CVE-2022-36771](#)
 - [CVE-2022-24785](#)
 - [CVE-2022-2191](#), [CVE-2022-2047](#), [CVE-2022-2048](#), [CVE-2022-24823](#), [CVE-2020-36518](#)
- Updated the Rules and tuning for the UBA app topic and added a new topic for [“Machine learning analytic requirements” on page 270](#).

What's new in 4.1.8 (Released August 2022)



Attention: Starting with UEBA 4.1.8, support is limited to QRadar versions 7.4.3+.

- Fixed an issue with dashboard views showing counts that also included deleted users.
- Improved upgrade process for UEBA and Machine Learning
- Added Time to Live element to UBA : Dormant Account ref set.
- Updated machine learning models to use the Bytes Sent and Bytes Received.
- Updated API calls to support the newer versions of QRadar.
- Fixed name display for HTTP Data model on the User profile page.
- Fixed name display for Username on the UEBA Dashboard page.
- Because of a limitation with QRadar APIs, the following will no longer be monitored in UEBA:
 - Usernames that have a leading . or \$
 - Usernames that contain any of the following special characters: <>?*+=+,;:[]
- Fixed some security vulnerabilities. For more information, see the following security bulletins:
 - [CVE-2021-4104](#)
 - [CVE-2021-41182](#), [CVE-2021-41183](#), [CVE-2021-41184](#), [CVE-2021-23445](#), [CVE-2021-29489](#)

What's new in 4.1.7 (Released March 2022)

- Fixed an issue that caused incorrect navigation to QRadar from UEBA on IBM Cloud Pack for Security.
- Fixed a deadlocking issue that caused user import failures.
- Fixed an issue that was preventing user imports from writing data to the reference table.
- Fixed an issue that caused database migration failures when upgrading.
- Fixed an issue with Machine Learning that showed the space available status as 0.

Known issue: Because of the changes implemented to fix issues with user imports in UBA 4.1.7, performance during coalescing might be slow. Consider decreasing the number of aliases to reduce performance impact.

What's new in 4.1.6 (Released 7 January 2022)

- Updated the ncurses library to version 6.1.9.
- Fixed a security vulnerability. For more information, see the following security bulletin: [CVE-2021-45105](#).

What's new in 4.1.5 (Released 17 December 2021)

UEBA 4.1.5 includes the following updates:

- Addressed an issue with migrating an older version of PostgreSQL database during some upgrade scenarios.
- Fixed some security vulnerabilities. For more information, see the following security bulletins:
 - [CVE-2021-44228](#)
 - [CVE-2021-45046](#)

What's new in 4.1.3 (Released 09 December 2021)

UEBA 4.1.3 includes the following updates:

- Improved User imports so that you can use more special characters for Custom attributes.

- Improved the navigation with QRadar Analyst Workflow integration if QRadar Analyst Workflow is installed.

What's new in 4.1.2 (Released 30 July 2021)

UBA 4.1.2 includes the following updates:

- Improvements to coalescing
- Improvements to AQL filtering operations
- Updates to QRadar Use Case Manager integration
- Fixed a security vulnerability. For more information, see the following security bulletin: [CVE-2021-29757](#).
- Added the following MaaS360 use cases:
 - UBA : MaaS360 malicious URL accessed. For more information, see [“UBA : MaaS360 malicious URL accessed”](#) on page 220.
 - UBA : MaaS360 malware application installed. For more information, see [“UBA : MaaS360 malware application installed”](#) on page 220.
 - UBA : MaaS360 URL access blocked. For more information, see [“UBA : MaaS360 URL access blocked”](#) on page 219.
 - UBA : MaaS360 malicious email received. For more information, see [“UBA : MaaS360 malicious email received”](#) on page 219.
 - UBA : MaaS360 malicious SMS received. For more information, see [“UBA : MaaS360 malicious SMS received”](#) on page 218.
 - UBA : MaaS360 device out of compliance due to OS version. For more information, see [“UBA : MaaS360 device out of compliance due to OS version”](#) on page 218.
 - UBA : MaaS360 device out of compliance due to encryption level. For more information, see [“UBA : MaaS360 device out of compliance due to encryption level”](#) on page 217.
 - UBA : MaaS360 device out of compliance due to device being rooted. For more information, see [“UBA : MaaS360 device out of compliance due to device being rooted”](#) on page 217.
 - UBA : Potential Access to Blocklist Domain. For more information, see [“UBA : Potential Access to Blocklist Domain”](#) on page 225.
 - UBA : MaaS360 detected device with low encryption level. For more information, see [“UBA : MaaS360 detected device with low encryption level”](#) on page 216.

What's new in 4.1.1 (Released 10 May 2021)

UBA 4.1.1 includes the following updates:

- For QRadar on Cloud deployments, you can now install Machine Learning in application dense environments as the installation is no longer restricted to 10% of memory.
- For QRadar on Cloud deployments, the Learned peer group model no longer requires an App Host.
- Fixed an issue with User imports that caused duplicate users in UEBA.
- Fixed an issue that prevented PSQL migration when UEBA data had been cleared. For more information, see [QRadar: Upgrading to UBA 4.1.0 can lead to aspects of the app not functioning properly](#).
- Fixed an issue where Ariel Searches were not deleted and the User Details Event Viewer showed “No results found for AQL query”.
- Fixed issues where rule name and event name changes were breaking the Rules and Tuning page.
- Added public API documentation. For more information, see [“Public API documentation for UEBA”](#) on page 277.

- Integration with QRadar Use Case Manager 3.2.0. UEBA rules are now managed in QRadar Use Case Manager 3.2.0 and later. For more information, see [“Integration with Use Case Manager 3.2.0 and later” on page 11.](#)
- Fixed some security vulnerabilities. For more information, see the following security bulletins:
 - [CVE-2021-20393](#)
 - [CVE-2021-20392](#)
 - [CVE-2021-20391](#)
 - [CVE-2021-20429](#)

What's new in 4.1.0 (Released 10 March 2021)



Attention: For the best experience, you should install 4.1.0 on the following QRadar versions:

- 7.3.3 Fix Pack 6 or later
- 7.4.2 Fix Pack 3 or later
- 7.4.3 or later

For multitenancy, UEBA version 4.1.0 is supported only on the following QRadar versions: 7.4.2 Fix Pack 3 or later and 7.4.3 or later.

Upgrade note: You should upgrade to UBA 4.0.1 (QRadar 7.3.3 or later) before you upgrade to UBA 4.1.0.

- Starting with 4.1.0, the Reference Data Import - LDAP (LDAP) app is no longer supported. You can import users with the User Imports wizard.
- Improved the Username display (under Monitored users) on the UEBA Overview page and removed tooltips. You can now click a username and open the user details panel that contains the information that was previously in a tooltip. For more information, see [“User details panel” on page 9.](#)
- Added the ability to create custom attributes with the User Imports wizard. For more information, see [“Custom attributes in the User imports wizard” on page 9.](#)
- Added the ability to delete a user from the user import and not just the user import configuration. For more information, see [“Deleting a user from the user import configuration” on page 9.](#)
- Added the ability to remove users that were discovered from events. For more information, see [“Remove users discovered from events” on page 10.](#)
- Added the ability to remove an alias and then recoalesce in the **User import > Tuning page**. For more information, see [“Removing an alias when you tune a user import” on page 10.](#)
- Updated the Help and Support page. For more information, see [“Updated Help and support page” on page 11.](#)
- Added the following use cases:
 - UBA : Executive only asset accessed by non-executive user from external network. For more information, see [“UEBA : Executive only asset accessed by non-executive user from external network” on page 88.](#)
 - UBA : Executive only asset accessed by non-executive user from internal network. (formerly called UBA : Executive Only Asset Accessed by Non-Executive User). For more information, see [“UEBA : Executive only asset accessed by non-executive user from internal network” on page 88.](#)
 - UBA : Multiple blocked file uploads followed by a successful upload. For more information, see [“UEBA : Multiple blocked file uploads followed by a successful upload” on page 198.](#)
 - UBA : Large number of denied access events towards external domain. For more information, see [“UEBA : Large number of denied access events towards external domain” on page 91.](#)
 - UBA : Remote access hole in corporate firewall. For more information, see [“UEBA : Remote access hole in corporate firewall” on page 93.](#)

User details panel

You can click a username to open the User details panel that shows you details about the user including overall risk, display name, top 3 anomalies, watchlists, and aliases. To open the full User details page, click **View user details**.

The screenshot displays the QRadar interface with the User details panel open for user 'ibm_sense_ml-3'. The main dashboard shows the following metrics:

- Monitored users: 450.7k
- High risk users: 205 (0% of monitored users)
- Users discovered from events: 425.5k (94% of monitored users)
- Users imported from direct: 25.2k (6% of monitored users)

The User details panel for 'ibm_sense_ml-3' includes:

- Overall risk: Critical 1,627.1
- Display name: ibm_sense_ml-3
- Top 3 of 28 anomalies detected:
 - Feb 18 12:44 PM - 1:44 PM (60 minutes): UBA : Abnormal increase in Risk activity
 - UBA : Abnormal Volume of Data Downloaded
 - UBA : Abnormal increase in DOS activity
- Watchlists (1): IBM Sense Users
- Aliases (1): Never Used
- View user details button

Custom attributes in the User imports wizard

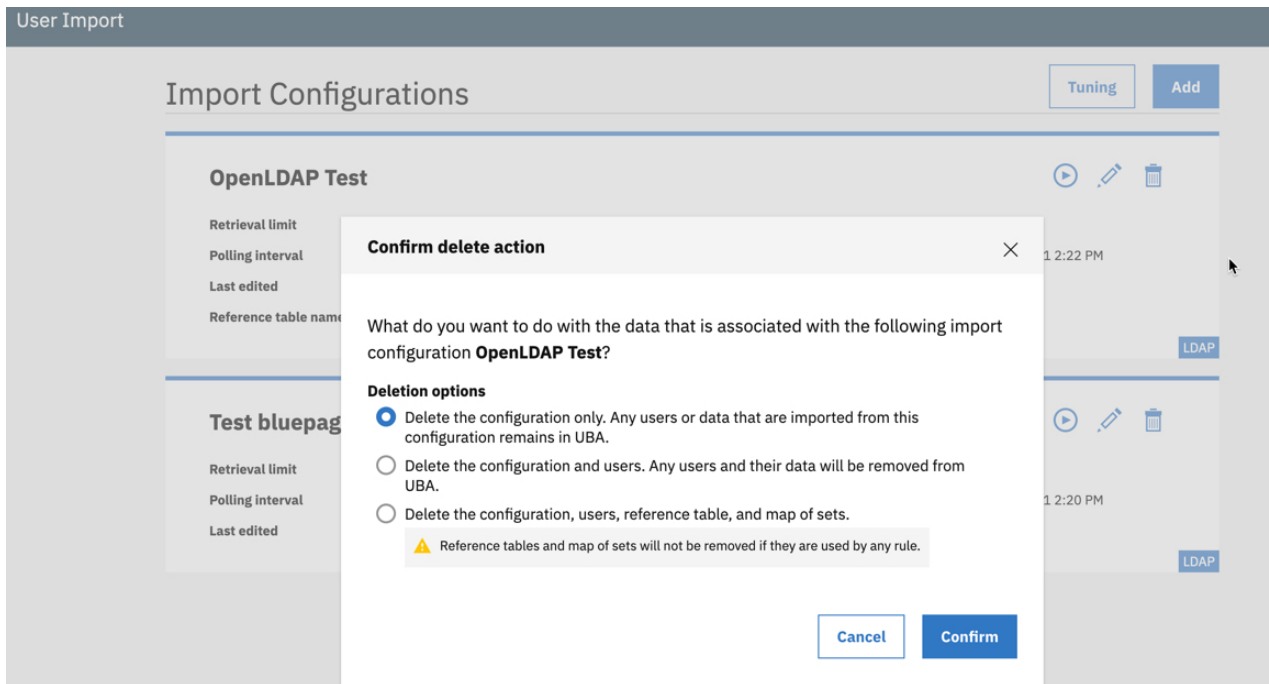
You can create custom attributes when you tune your user imports with the User imports wizard. For more information, see [“Tuning user import configurations”](#) on page 41.

The screenshot shows the 'Custom attributes' configuration page. The breadcrumb navigation is: Overview / User import / Tuning / Custom attributes. The page title is 'Custom attributes'. Below the title, there is a description: 'Create custom attributes by combining existing attributes that can be selected on the Edit panel from the tuning page. Note: Combining imported attributes can take several hours depending on the number of users. The selected aliases or display fields will display on the profile page when coalescing is complete.' A blue 'Add new' button is highlighted with a red box. Below the button, there is a note: 'Click "Add new" to add the first custom attribute.' At the bottom right, there are 'Cancel' and 'Save' buttons.

Deleting a user from the user import configuration

When you delete a User import configuration, you now can choose to delete only an import configuration or you can choose to delete the users (and their data) who are associated with the selected user import configuration.

Note: If you selected the **Synchronize reference table** option when you configured the import, you will have the option to **Delete the configuration, users, reference table, and map of sets**.



Removing an alias when you tune a user import

On the **User imports > Tuning** page, you can click **Edit** to open the Edit: Aliases page in the User coalescing section. You can select the "x" to remove an alias to uncoalesce (separate combined users) that you have previously coalesced. When you remove an alias it then recoalesces. Note that when you delete an alias it takes effect only when the value of that alias is not shared with the deleted imports.

Edit: Aliases

Select the attributes from the current imports, which UBA can use to identify and combine activity from different usernames of each user. Do not select attributes that have shared values across users. Selecting a shared attribute, such as department or country, causes UBA to combine all users with the same department or country value.

Selected attributes

uid x samaccountname x mail x dn x notesmailfile x

Remove users discovered from events

In the Administrative functions section on the Help and support page, you can remove only users that were discovered from events. You can click to see the users that were discovered from events and that will be removed. After confirming the user removal, the count on the overview page under Users discovered from events should decrease to zero.

Tip: You should enable the **Monitor imported users only** option on the UBA Settings page before removing event users if you don't want to discover users from events again.

Selecting **Remove event users** does not remove users that you imported.

Administrative Functions

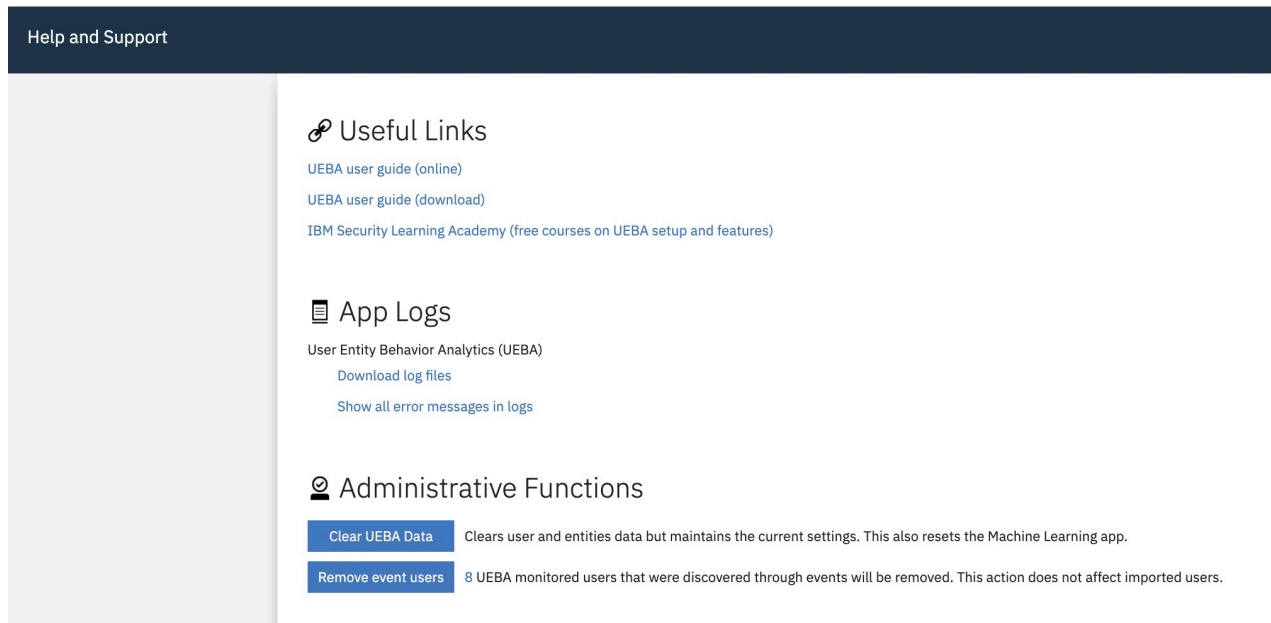
Clear UBA Data	Clears UBA user data but maintains the current settings. This also resets the Machine Learning app.
Remove event users	30 UBA monitored users that were discovered through events will be removed. This action does not affect imported users.

Integration with Use Case Manager 3.2.0 and later

When you upgrade to UBA 4.1.0 (and later) and Use Case Manager 3.2.0 and later, you manage rules in Use Case Manager and no longer manage rules in the UBA Rules and Tuning page. For more information, see [QRadar Use Case Manager](#).

Updated Help and support page

The following image shows an example of the updated Help and Support page for 4.1.0.



Related concepts

[“Earlier versions” on page 11](#)

In case you missed a release, review a list of features from previous versions.

Earlier versions

In case you missed a release, review a list of features from previous versions.

What's new in 4.1.16

- RBAC (Role Based Access Control) Feature - Client can take leverage of role based access of the User Entity Behavior Analytics (UEBA) functionality. RBAC is divided into three roles namely, **Admin**, **Tenant admin** and **Read-only**.
- Upgraded the app base image to v3.0.11.
- Upgraded the java version of the machine learning app to v17.0.7.
- Fixed security vulnerabilities.

What's new in 4.1.15

- Updated the ncurses library to v6.1.10.

What's new in 4.1.14

- UEBA now displays the tenant name in the UEBA header area if multi-tenant configuration is detected.
- UEBA now provides options to select and delete multiple users at once on the search results page.
- UEBA now uses the correct IP address when the Encrypted App host is used in the NAT environment.
- Improved ML to use the correct IP address when the Encrypted App host is used in the NAT environment.
- The ML model now recovers if the build fails with error - "*lost user Id lookup object*".
- Added more files that are gathered by using the ML download logs function on the UEBA help or support page.
- Fixed an issue in UEBA triggering an unexpected error state when you are viewing the user details in the IBM QRadar Security Orchestration Automation and Response (SOAR) App.
- Fixed an issue where a query on a custom model in ML fails validation if that query contained the character sequence '\$'.
- Fixed an issue that crashed the **UBAController** process when a configuration is saved and if it is existing in the zookeeper.

What's new in 4.1.13

- Decay risk factor can now be set to zero, which disables reducing the overall risk score for users.
- Error messages that are related to installing or uninstalling the machine learning is now displayed for 30 seconds on the installer page.
- Fixed an issue that was preventing proper redirection to the Use-case Manager when you are viewing a tenant instance of UEBA when logged in as an admin.
- Fixed an issue where the use of **View User Details** on the username fields that contained N/A in QRadar that matched random users.
- Fixed an issue that prevented the failed machine learning models to self-correct.
- Fixed security vulnerabilities.

Known issues

The QRadar User Entity Behavior Analytics app has required information for upgrading and known issues.

Known issues

The QRadar User Entity Behavior Analytics app has the following known issues:

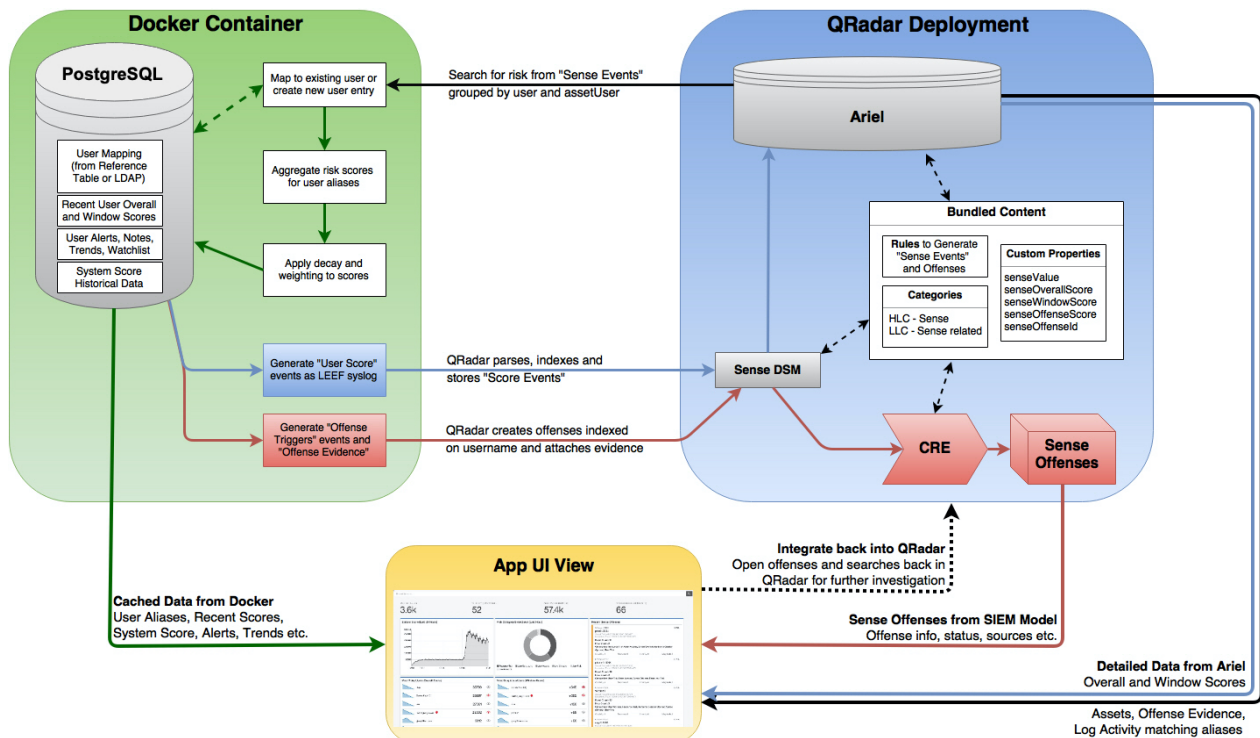
- When you try to install User Entity Behavior Analytics 4.1.17 on QRadar 7.5.0 Update Package 10 or later, you see an error message that the application is not supported. The workaround is to update the minimum permitted app base image stream in QRadar.
 1. Go to **Admin > System Settings > Minimum Permitted App Base Image Stream**.
 2. Change the version from **v4+ (RHEL with Python 3.11)** to **v3+ (RHEL with Python 3.8)**, and then deploy the changes.
- In User Entity Behavior Analytics 4.1.13 and later, the QRadar APIs make repeated calls to determine whether User Entity Behavior Analytics is running on a QRadar on Cloud instance. These calls result in numerous API failure messages in the audit logs.
- In User Entity Behavior Analytics 4.1.7 and 4.1.8, if you select **Generate map of sets** when importing users with LDAP or Active Directory, you might experience a timeout failure with larger data sets. This

is due to a problem in the **api/reference_data/map_of_sets/bulk_load/** QRadar API endpoint that is taking progressively longer times to return a status when called as the data in the table grows.

- Because of the changes that are implemented to fix issues with user imports in User Entity Behavior Analytics 4.1.7, performance during coalescing might be slow. Consider decreasing the number of aliases to reduce performance impact.
- In 4.0.0 and later, the User Entity Behavior Analytics dashboard might be slow to display the Active Analytics on some QRadar systems.
- Enabling **Search assets for username, when username is not available for event or flow data** on the **UBA Settings** page can cause the **User Details** page to not load. Review the Rules pages to determine whether the enabled rules require this setting. Disable the setting if it is not needed.
- In previous releases, new users were designated to User Entity Behavior Analytics in a way that used the "UBA : User Accounts, Successful, Observed" reference set. This reference set is no longer used. If you are experiencing performance issues because of the reference set after upgrading to V3.5.0 or later, consider deleting the data from the reference set. Also, if you previously edited the "UBA : New Account Use Detected" rule, consider reverting it back to the default setting to get the newer version.
- If you are upgrading the User Entity Behavior Analytics app and you receive a QRadar Notification exception error stating that a rule set has failed to load, you can ignore it and continue. If the error persists, contact IBM Customer Support.
- After you upgrade User Entity Behavior Analytics, the **Machine Learning Activity Distribution** graph on the **User Details** page can take up to one day to display.

Process overview

The UEBA app works with your QRadar system to collect data about the users inside your network.



How UEBA works

1. Logs send data to QRadar.
2. UEBA specific rules look for certain events (depending on which UEBA rules are enabled) and trigger a new sense event that is read by the UEBA app.

3. The UEBA rules require the events to have a username and other tests (review the rules to see what they are looking for).
4. UEBA pulls the *senseValue* from a reference table and the username from the sense event and then increases that user's *risk score* by the *senseValue* amount.
5. When a user's *risk score* exceeds the threshold that you set in the UEBA Settings page, UEBA sends an event which triggers the "UBA : Create Offense" rule and an offense is created for that user.

Risk score

A risk score is the summation of all risk events that are detected by UEBA rules. The higher the risk score, the more likely an internal user is to be a security risk and warrants further review of the user's network activity. The risk score reduces over time if no new events occur. The amount of the reduction is controlled from the value in **Decay risk by this factor per hour** on the UEBA Settings page.

How senseValues are used to create user risk scores

Each rule and analytic has a value assigned to it that indicates the severity of the issue found. Each time a user's actions causes a rule to trigger, the user gets this value added to the score. The more the user "violates" a rule, the higher the score will be.

Rules and sense events

Rules, when triggered, generate sense events that are used to determine the user's risk score.

You can update existing rules in QRadar to produce sense events. For more information, see [“Integrating new or existing QRadar content with the UEBA app”](#) on page 62.

Machine Learning Analytics and sense events

You can install the Machine Learning Analytics app and enable machine learning analytics to identify anomalous user behavior. The analytics, when triggered, will generate sense events that also raise a user's risk score.

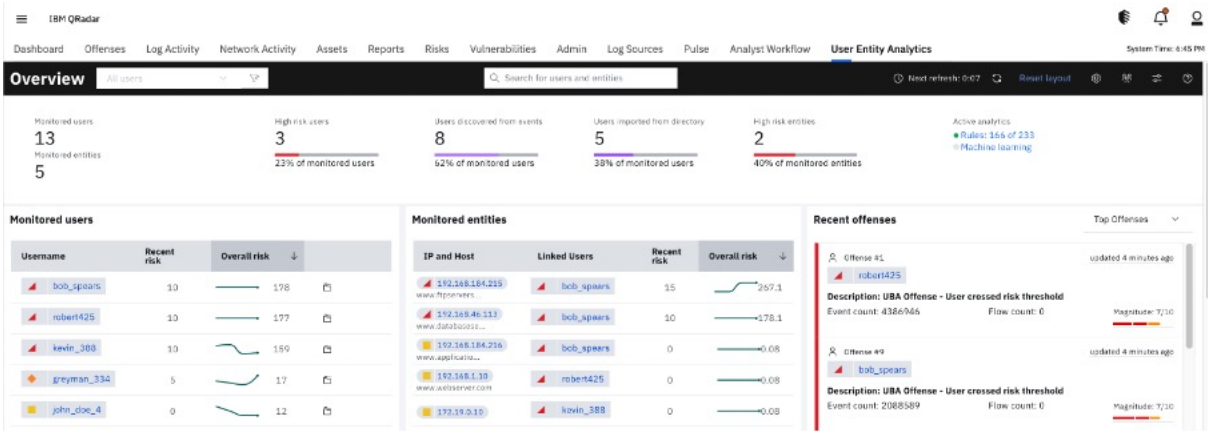
Entity overview

Starting UEBA 5.x UEBA now also monitors risky entities in the environment. Entities could be a device or an asset like a database server, firewall or endpoint.

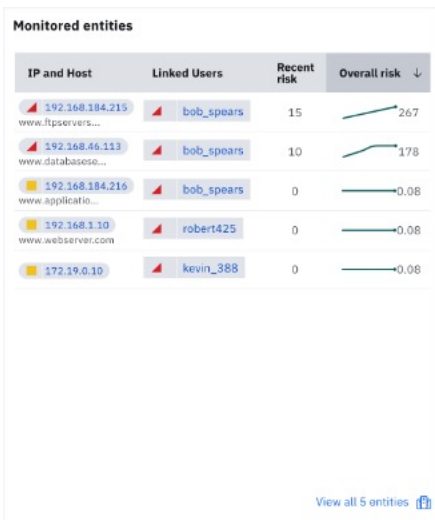
UEBA uses asset database component that discovers and maintains asset information such as IP address, hostname, vulnerability score (if supported scanner data is connected). See entity tuning section to ensure Assets are up to date.

The UEBA dashboard now shows **Monitored Users** and **Monitored Entities**.

The top panel in the dashboard shows total monitored entities and total high risk entities in the environment.



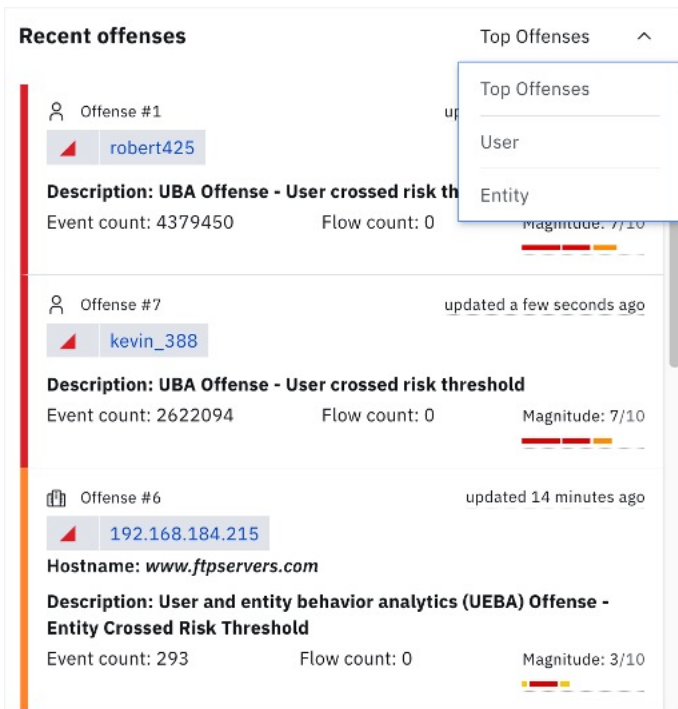
Monitored Entity widget adds entity specific information to give a quick view of risky device IP address, hostname, linked users, recent risk and overall risk of those risky devices.



Entity offenses

If the entity or a device risk goes beyond the configure threshold value, UEBA will generate an Offense for further investigation.

Offense widget in dashboard now has a drop-down menu to select user or entity offenses.



Risk entity summary

You can click an entity in the UEBA dashboard to view the following information.

- Overall risk
- Anomalies detected in last 30 minutes
- Linked users

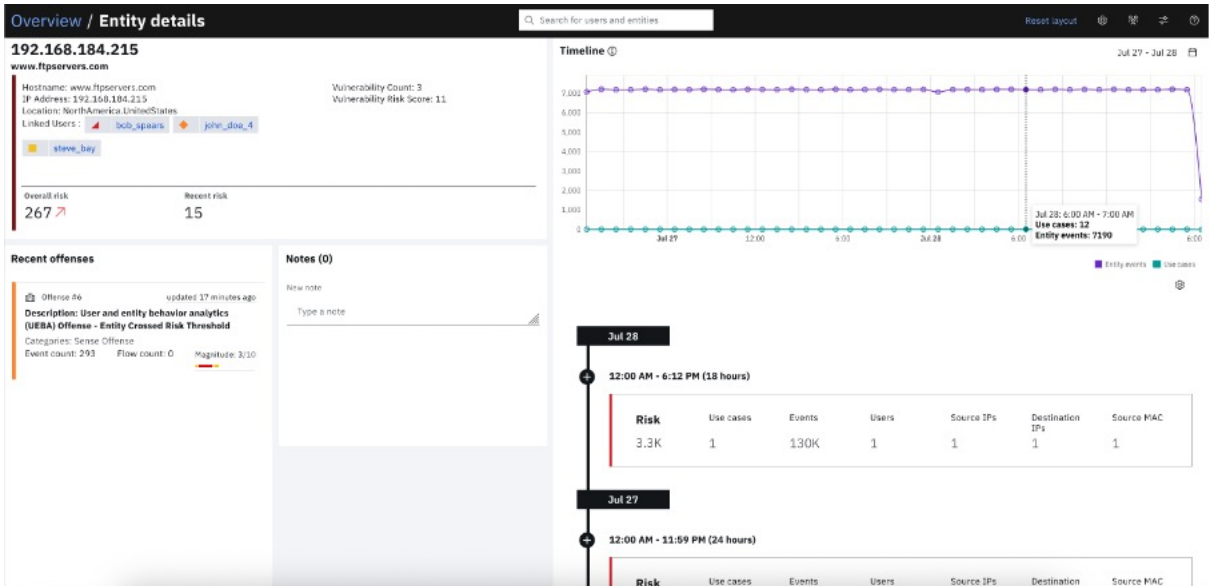
Entity details

You can click **View entity details** to view entity details.

- IP address
- Hostname
- MAC address
- Location
- Linked users
- Vulnerability count
- Vulnerability Risk Score

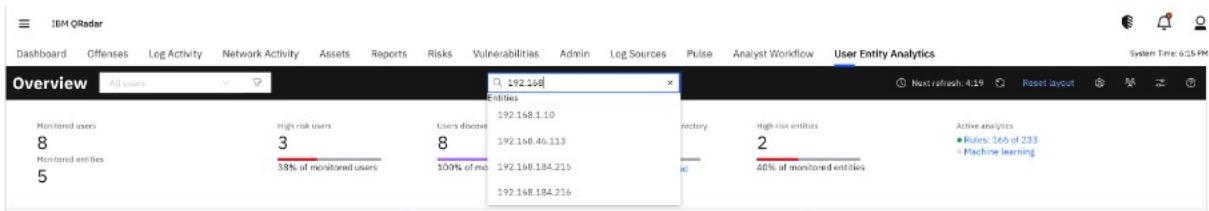
Vulnerability count and Vulnerability Risk Score are shown when a supported VA scanner data is connected to QRadar.

Timeline for entity is provided to drill down for further investigation.



Searching for entities

You can use the UEBA dashboard search bar to search for any monitored entities in UEBA.



UEBA overview and user details

The IBM QRadar User Entity Behavior Analytics (UEBA) app shows you the overall risk data for users in your network.

Overview page

After you install and configure the UEBA app, open the UEBA Overview (Dashboard) page.

Note: The supported number of users that the UEBA app can monitor is 400,000 users.

In the **Viewing: All users** field, you can create and select views to customize your dashboard view. For more information, see [“Managing the UEBA dashboard views”](#) on page 22.

In the **Search** field, you can search for users by name, email address, user name. As you enter a name, the app shows you the top five results.

The **Tenant** label shows the domain name of the current tenant being viewed.

The risk level for each user is indicated by an icon. The yellow square icon (low) shows when risk is 25% or less of the risk threshold. The orange diamond (medium) shows when risk is at 50% of the risk threshold. The red pyramid (high) shows when risk is at 75%. The red triangle (critical) shows when risk is at 100% or more.

The dashboard is automatically refreshed every minute and shows you the following risk data:

Table 1. UBA dashboard data

Dashboard settings	Description
Monitored Users	Displays the total number of users that the UEBA app is actively monitoring.
Monitored Entities	Displays the total number of entities that the UEBA app is actively monitoring.
High Risk Users	Displays the number of users who are currently exceeding the risk score. The value for determining the risk score is set in the "Risk threshold to trigger offenses" in UEBA Settings.
Users Discovered from Events	Displays the number of users that are discovered from events, excluding imported users.
Users Imported from Directory	Displays the number of users that were imported from reference tables.
High Risk Entities	Displays the number of entities that are currently exceeding the risk score. The value for determining the risk score is set in the "Risk threshold to trigger offenses" in UEBA Settings.
Active Analytics	<ul style="list-style-type: none"> • Rules: Indicates the status of the rules content and how many rules are active. A green status indicates that the rules are installed and active. Gray indicates that the rules are disabled. Yellow indicates that the installation is in progress. Click to open the Rules and Tuning page. Note: In a multitenant environment, only an Admin user can see the rules installation status for either admin or tenant UBA. Tenant admin and tenant user always see a green status of rules on the dashboard. • Tip: The rule count is based on the total number of rules that UBA knows exist, regardless of whether the rules are installed or not. Use Case Manager filtering is based on what is installed. For more information, see "Supported QRadar content" on page 232. • Machine Learning: Indicates the status of Machine Learning and how many models are active. A green status indicates that the Machine Learning Analytics app is installed. Gray indicates that the Machine Learning Analytics app is not installed. Click to install or configure Machine Learning. Note: In a multitenant environment, the status is always Green.
Monitored users	<p>Displays the top 10 riskiest users. Click a username to view available details on the User details panel.</p> <ul style="list-style-type: none"> • Recent risk: Shows the accumulated risk for the respective user for the last 5 minutes. • Overall risk: Shows a line graph that illustrates the user's overall risk score trend for the last hour. The color of the graph indicates the overall riskiness. • Watchlist icon: Add the user to a watchlist or create a watchlist. The number indicates how many watchlists the user is a member of. • You can view all the tracked users on the Search page.
Recent offenses	Displays last five most recent offenses that are sorted by the time the offense was last updated.

Table 1. UBA dashboard data (continued)

Dashboard settings	Description
[User] Watchlist	<p>Watchlists that you created. You can create as many watchlists as you want and they display on the Dashboard. You can view all the tracked users in the custom watchlist that you created on the Search page.</p> <p>Tip: To add a user to a watchlist, click the Watchlist icon.</p> <p>The number indicates how many watchlists the user is a member of.</p>
System score	<p>Overall accumulated risk score for all users at a specified point in time. Click the Calendar icon to specify a date range for longer than one day. The maximum duration that you can select is 30 days any time during the last year. Note: If you are viewing a custom dashboard view, the System Score graph is not shown.</p>
Risk category breakdown	<p>High-level risk categories over the last hour. Click the graph to see subcategories and then click to see a display of events. Click the Table view icon to view the same information in a table format. Note: If you are viewing a custom dashboard view, the Risk category breakdown graph is not shown.</p>
Users with dormant accounts	<p>Watchlist of users that are flagged as having dormant accounts. The Users with Dormant Accounts is automatically generated.</p>
Active investigations	<p>Users that are currently under investigation. Select the My investigations checkbox to show only those investigations that you started.</p>
Status of machine learning models	<p>Status of the Machine Learning Analytics is visible if the Machine Learning app is installed. For more information, see “UEBA dashboard with Machine Learning” on page 241.</p>

User details page

You can click a user name from anywhere in the app to open the User details panel and see details for the selected user. To open the full User details page, click **View user details** on the panel.

You can learn more about the user's activities with the *event viewer* pane. The event viewer pane shows information about a selected activity or point in time. Clicking an event in the *event viewer* pane reveals more details such as syslog events and payload information. The event viewer pane is available for all donut and line graphs and activities in the Risky Activity Timeline on the **User details** page.

The **User Details** page includes the following user information:

- Shows the name and aliases of the selected user and any additional details from attributes (including domain, manager, and peer information) that are imported from LDAP.
- Shows the status (dormant, active, never used) of all the accounts that are found to be associated with the user.
- If you have IBM QRadar Advisor with Watson 2.5.2 or later installed, you can search for information that is related to the user. You must have QRadar administrator privileges. Click the **Search Watson** icon.
- To initiate an investigation on the user, click the **Start Investigation** icon. When your investigation is complete, click the **End Investigation** icon.
- To add the user to a watchlist or create a watchlist, click the **Watchlist** icon.

The **Advanced actions** list includes the following actions:

Table 2. Advanced actions list

Advanced actions	Description
Add custom alert	You can set a custom alert that is displayed by the user name. Click Add Custom Alert , enter an alert message, and then click Set . To remove the custom alert for the selected user, click Remove Custom Alert .
Add to trusted users list	You must have QRadar administrator privileges. You can add the selected user to the trusted users list so that the user does not generate risk scores and offenses. To remove the selected user from the list, click Remove from trusted users list . To review the complete list of users who were added to the list, see “Viewing the trusted users list” on page 52.
Generate GDPR compliant report for user	You can generate a General Data Protection Regulation (GDPR) compliance report for the user. Important: Generate the report before you click Delete and stop tracking user .
Delete and stop tracking user	You must have QRadar administrator privileges. You can click Delete and stop tracking user to comply with General Data Protection Regulation (GDPR). Select Yes to permanently delete and stop tracking the user. To begin tracking the user again, delete the user's aliases from the <i>UBA : Users Not Tracked</i> reference set. To view all the user's aliases, download the GDPR report before you delete the user. For more information about the <i>UBA : Users Not Tracked</i> reference set, see “Reference sets” on page 69.
Always track with Machine Learning	You must have QRadar administrator privileges. You can click Always track with Machine Learning to add the user to the <i>UBA: ML Always Tracked Watchlist</i> reference set. Adding the user to the reference set provides the highest likelihood that the user is included in a machine learning model. For more information about reference sets in UBA, see “Reference sets” on page 69. To remove the selected user from the reference set, click Tracked with Machine Learning .

testuser_32

Full name: testuser_32
 Email: testuser_32@ibmemm.edu
 Job title: Your Highness (200 peers)
 Manager: cn=Bill Lumbergh,ou=People,dc=u... (200 peers)
 Domain: [ibmemm.edu](#) (200 peers)

Overall risk: 0 — Recent risk: 0

Advanced actions

- Add custom alert
- Add to trusted users list
- Generate GDPR compliant report for user
- Delete and stop tracking user
- Always track with machine learning

You can view the following information about the selected user:

Table 3. User details settings

User details	Description
Overall Risk Score	The overall risk score shows the risk trends for the user.

Table 3. User details settings (continued)

User details	Description
Timeline	<p>The timeline graph shows Use cases and User events. Use cases are events that contribute to risk score. User events are all events triggered by the user. The Y-axis is event count and X-axis is time. You can click any activity in the timeline to open the event viewer pane that lists supporting log events that are associated with the user's activity. Click an event to view more details such as syslog events and payload information.</p> <ul style="list-style-type: none"> • Timeline activity is grouped by sessions and days. Sessions are defined in the Application Settings section of the UBA Settings page. The colors represent the overall riskiness of a session. Click the Calendar icon to specify the date range (1 - 14 days). • You can customize the metric settings that display for the timeline by clicking the Metric Settings icon. You can add and remove the categories that you want to see. The data shown in the Example metrics section of the Metric Settings screen does not represent real values.
Recent Offenses	Shows any user type offense, where the user name matched any of the selected user's aliases. The last five offenses are displayed. Click an offense to open the Offenses tab in QRadar.
Risk Category Breakdown	Shows the risk categories of the selected user during the last hour.
Notes	<p>Type a note in the in New note section to add a note for the selected user. The notes are automatically deleted after the 30-day retention period.</p> <p>Note: To save the note indefinitely, click the Keep forever icon.</p>

You can configure some machine learning graphs to display on the User Details page if the Machine Learning Analytics app is installed and the specified model is enabled. For more information, see [“UEBA dashboard with Machine Learning”](#) on page 241.

To return to the main UBA Overview page, click **Overview**.

Related concepts

[“UEBA dashboard with Machine Learning”](#) on page 241

The IBM QRadar User Entity Behavior Analytics (UEBA) app with Machine Learning Analytics includes the Machine Learning model status and additional details for the selected user.

[“Dormant accounts”](#) on page 55

You can see users in your system that have dormant accounts, active accounts, or accounts that have never been used.

Related tasks

[“Creating watchlists”](#) on page 48

You can add and configure watchlists that include user-based members, entity-based members, and hybrid watchlists that combine both user and entity memberships.

[“Viewing the trusted users list”](#) on page 52

You can view the list of trusted users in the reference set management list.

[“Adding log sources to the trusted log source group”](#) on page 54

If you do not want the IBM QRadar User Entity Behavior Analytics (UEBA) app to monitor and report certain log sources, you can add them to the **UBA : Trusted Log Source Group**. Adding log sources to the group stops the UBA app from monitoring them.

[“Installing the Machine Learning Analytics app”](#) on page 240

As a QRadar Admin, you can install the Machine Learning Analytics (ML) app after you have installed the QRadar User Entity Behavior Analytics (UEBA) app from the Extension Manager.

[“Investigating users in QRadar Advisor with Watson” on page 23](#)

You can select users from the QRadar User Entity Behavior Analytics (UEBA) app to send to QRadar Advisor with Watson for investigation.

Managing the UEBA dashboard views

You can customize UEBA dashboard views, including light or dark mode, and filter on attributes that include domain, city, country, or state from a user import.

Before you begin

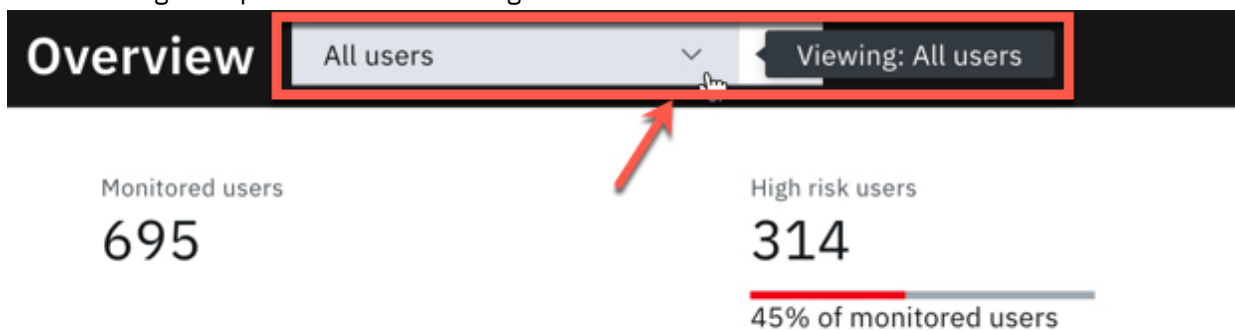
You must install, configure, and import users into the UEBA app that contain location or domain data.

About this task

You must have Admin permissions to manage the dashboard views. The dashboard views are not available if there are no imported users that contain location or domain data.

Procedure

1. Select the **User Entity Analytics** tab.
2. On the main UEBA Overview (Dashboard) page, from the filter box, click **Viewing: All users**. The following example shows 4.0.0 with light theme UI.



3. Click the **Manage dashboard views** icon. The following example shows 4.0.0 with light theme UI.



4. On the **Manage dashboard views** screen, create or edit views to filter the users that are displayed on the UEBA Overview (Dashboard) page.
5. For each view you want to create, enter the following information:
 - **View name:** Enter a descriptive name for each view. For example, "US employees".
 - **Attribute:** Select from domain, state, country, or city.
 - **Value:** Select one or multiple values based on the attribute selection.

The following example shows 4.0.0 with light theme UI.

Create and edit views to filter the users that are displayed on the UBA dashboard.

Create new view

View name	Attribute	Value
ATL	city	Atlanta,Georgia,United States (7 users)
GA	state	GA (7 users)
LVille	city	Lawrenceville,GA,US (7 users)
US	country	United States (54 users) US (12 users)

Cancel Save

6. Click **Save**.

7. To create another view, click **Create new view**. Note that you can create up to 30 views. The views that you create are available from the filter box in step 2.

Investigating users in QRadar Advisor with Watson

You can select users from the QRadar User Entity Behavior Analytics (UEBA) app to send to QRadar Advisor with Watson for investigation.

Before you begin

- You must have User Entity Behavior Analytics (UEBA) app 3.5.0 or later installed and configured with user data.
- You must have Admin privileges.
- You must have QRadar Advisor with Watson 2.5.2 or later.

For more information, see [QRadar Advisor with Watson](#).

Procedure

1. Click the **User Entity Analytics** tab to open the UEBA **Dashboard**.
2. Select a user or search for a user to open the **User Details** page.
3. Click the **Search Watson** icon.

When the icon stops spinning, the Watson Investigations ID details page opens and you can review your results in the QRadar Advisor with Watson app.

Prerequisites for installing the User Entity Behavior Analytics app

Before you install the User Entity Behavior Analytics (UEBA) app, ensure that you meet the requirements.

- Verify that you have IBM Security QRadar 7.4.3 Fix Pack 6 or later installed.
- Add the IBM Sense DSM for the User Entity Behavior Analytics (UEBA) app.

Installing the IBM Sense DSM manually

The User Entity Behavior Analytics (UEBA) app uses the IBM Sense DSM to add user risk scores and offenses into QRadar. You can install the DSM through auto-updates or you can upload to QRadar and install it manually.

Note: If your system is disconnected from the internet, you might need to install the DSM RPM manually.

Restriction: Uninstalling a Device Support Module (DSM) is not supported in QRadar.

1. Download the DSM RPM file from the [IBM support website](#):
 - For QRadar 7.4.0 and later: `DSM-IBMSense-7.4-20200812144513.noarch.rpm`
2. Copy the RPM file to your QRadar Console.
3. Use SSH to log in to the QRadar host as the root user.
4. Go to the directory that includes the downloaded file.
5. Type the following command:

```
rpm -Uvh <rpm_filename>
```
6. From the **Admin** settings, click **Deploy Changes**.
7. From the **Admin** settings, select **Advanced** > **Restart Web Services**.

Log source types relevant to the UEBA app

The User Entity Behavior Analytics (UEBA) app and the ML app can accept and analyze events from certain log sources.

In general, the UEBA app and the ML app require log sources that supply a username. For UEBA, if there is no username, enable the **Search assets for username, when username is not available for event or flow data** checkbox in UEBA Settings so that UEBA can attempt to look up the user from the asset table. If no user can be determined, UEBA does not process the event.

For more details about specific use cases and the corresponding log source types, see [Chapter 8, “Rules and tuning for the UEBA app,”](#) on page 83.

Related tasks

[“Configuring UEBA settings”](#) on page 31

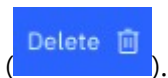
To view information in the IBM QRadar User Entity Behavior Analytics (UEBA) app, you must configure UEBA application settings.

Deleting users or entities from UEBA

You can remove one or up to 100 users or entities. from the QRadar User Entity Behavior Analytics (UEBA) app at once.

Procedure

1. You can see the **Search result** page after searching for users or entities. of your search criteria, such as searching for monitored users or entities.
2. Select the checkbox next to the users or entities. that you want to delete, and click the **Delete** icon



3. In the **Confirm multiple users or entities. deletion** window, click **Yes** to remove the selected user or entity from UEBA.

The deleted users are added to the reference set *UBA : Users Not Tracked* reference set. The deleted entities are added to the reference set *UEBA : Entities Not Tracked*.

For more information about the *UBA : Users Not Tracked* reference set, see [“Reference sets”](#) on page 69.

Chapter 2. Installing and uninstalling

Installing the User Entity Behavior Analytics app

Use the IBM QRadar Extension Management tool to upload and install your app archive directly to your QRadar Console.

Before you begin

Complete the [“Prerequisites for installing the User Entity Behavior Analytics app”](#) on page 23.

Before you install the app, ensure that IBM QRadar meets the minimum memory (RAM) requirements. The UEBA app requires 1 GB of free memory from the application pool of memory. The UEBA app will fail to install if the application pool does not have enough free memory.

If UEBA fails to install, then your application pool does not have enough free memory to run the IBM QRadar UEBA app. Consider adding an app host to your QRadar deployment. Because of the size of UEBA with Machine Learning, you should install or upgrade to a medium deployment environment at a minimum.

QRadar uses an App Host, which is a managed host, that is dedicated to running apps. App Hosts provide extra storage, memory, and CPU resources for your apps without impacting the processing capacity of your QRadar Console. For more information, see [App Host](#).

Important:

- If you are having rule-related or search related performance issues on your console or any of your Event Processors or Data Nodes, fix the issues before you install UEBA as installing UEBA could add additional rule processing and search load.
- Tune QRadar assets. For more information, see [Tuning entity assets](#)

About this task

UBA-specific content packages, which contain rules for triggering offenses, are now installed as separate extensions. Content packages are installed by default. If you choose to create your own custom rules to trigger offenses in UEBA, you can change the **Install and upgrade content packages** setting when you configure UEBA Settings.



Attention: After the app is installed, you must:

- Enable indexes
- Deploy the full configuration.
- Clear your browser cache and refresh the browser window.
- Set up permissions for users that require access to view the **User Entity Analytics** tab. The following permissions must be assigned to each user role that requires access to the app:
 - User Entity Analytics
 - Offenses
 - Log Activity
- Complete the procedures in [Chapter 6, “Tuning,”](#) on page 61.
- Complete the procedures in [“UEBA common challenges”](#) on page 64.

Procedure

1. Choose one of the following methods to download your app:

- If the IBM QRadar Hub app is configured on QRadar, use the following instructions to install *User Behavior Analytics: IBM QRadar Hub* (https://www.ibm.com/support/knowledgecenter/SS42VS_SHR/com.ibm.apps.doc/t_qradar_adm_assistant_download.html).
 - If the IBM QRadar Hub app is not configured, download the *User Behavior Analytics* app archive from the [IBM Security App Exchange](https://apps.xforce.ibmcloud.com/) (<https://apps.xforce.ibmcloud.com/>) onto your local computer. You must have an IBM ID to access the App Exchange.
2. If you downloaded the app from the App Exchange, complete the following steps:
 - a) On the QRadar Console, click **Admin > Extensions Management**.
 - b) In the **Extension Management** window, click **Add** and select the UBA app archive that you want to upload to the console.
 - c) Select the **Install immediately** checkbox.

Important: You might have to wait several minutes before your app becomes active.
 - d) To preview the contents of an app after it is added and before it is installed, select it from the list of extensions, and click **More Details**. Expand the folders to view the individual content items in each group.

If the app installed successfully, you see it listed as 'Installed' on the **Extensions Management** page of the **Admin** tab. If the app didn't install correctly, see [QRadar apps troubleshooting](#).
 3. From the **Admin** settings, click **System Configuration > Index Management** and then enable the following indexes:
 - High Level Category
 - Low Level Category
 - Username
 - senseValue
 4. From the **Admin** settings, click **Advanced > Deploy Full Configuration**.

Note: Content packages are installed after the UEBA installation completes and UEBA is configured. For more information, see [“UEBA content pack summary”](#) on page 83.

What to do next

- When the installation is complete, clear your browser cache and refresh the browser window before you use the app.
- Manage permissions for UEBA app user roles.

Related tasks

[“Enabling indexes to improve performance”](#) on page 61

To improve the performance of your IBM QRadar User Entity Behavior Analytics (UEBA) app, enable indexes in IBM QRadar.

[“Assigning user capabilities for the QRadar User Entity Behavior Analytics app”](#) on page 47

Administrators use the User Role Management feature in IBM QRadar to configure and manage user accounts. As an administrator, you must enable the User Entity Analytics, Offenses, and Log Activity permissions for each user role that is permitted to use the QRadar User Entity Behavior Analytics (UEBA) app.

Uninstalling the UEBA app

Use the IBM QRadar Extension Management tool to uninstall your application from your QRadar Console.

Before you begin

If you have Machine Learning Analytics (ML app) installed, you must uninstall the ML app from the Machine Learning Settings page before uninstalling the UEBA app from the Extension Management window.

If you do not remove the ML app before you uninstall UEBA, you must remove it using the interactive API documentation interface.

Procedure

1. On the QRadar Console, click **Admin > Extensions Management**.
2. On the **INSTALLED** tab of the **Extension Management** window, select User Entity Behavior Analytics app and click **Uninstall**.

When you uninstall an app, it is removed from the system.

3. The following content packages are installed when you configure the UEBA app. You must uninstall each content package to completely remove the app.
 - User Entity Behavior Analytics Access and Authentication Content
 - User Entity Behavior Analytics Accounts and Privileges Content
 - User Entity Behavior Analytics Browsing Behavior Content
 - User Entity Behavior Analytics Cloud Content
 - User Entity Behavior Analytics DNS Analyzer Content
 - User Entity Behavior Analytics Domain Controller Content
 - User Entity Behavior Analytics Endpoint Content
 - User Entity Behavior Analytics Exfiltration Content
 - User Entity Behavior Analytics Geography Content
 - User Entity Behavior Analytics Network Traffic and Attacks Content
 - User Entity Behavior Analytics Threat Intelligence Content

Chapter 3. Upgrading the UEBA app

To take advantage of new capabilities, defect fixes, and updated workflows, upgrade to new versions of QRadar User Entity Behavior Analytics (UEBA). Use the Extensions Management tool in IBM QRadar to upgrade your app, or use the IBM QRadar Hub app to upgrade. You must be an administrator to upgrade to new versions of the app.

Before you begin

Important: Before you upgrade the app, ensure that IBM QRadar meets the minimum memory (RAM) requirements. The UEBA app requires 1 GB of free memory from the application pool of memory. The UEBA app will fail to upgrade if the application pool does not have enough free memory.

About this task

Note: If you customized your dashboard layout in releases prior to 4.0.0, the UI will reset to the default layout when you upgrade.

Procedure

1. Choose one of the following methods to download your app:
 - If the IBM QRadar Hub app is configured on QRadar, use the following instructions to install *User Behavior Analytics*: [Downloading apps with the IBM QRadar Hub app](#).
 - If the IBM QRadar Hub app is not configured, download the *User Behavior Analytics* app archive from the [IBM Security App Exchange \(https://apps.xforce.ibmcloud.com/\)](https://apps.xforce.ibmcloud.com/) onto your local computer. You must have an IBM ID to access the App Exchange.
2. If you downloaded the app from the IBM Security App Exchange, complete the following steps:
 - a) On the QRadar Console, click **Admin > Extensions Management**.
 - b) In the **Extension Management** window, click **Add** and select the app archive that you want to upload to the console.
 - c) Select the **Install immediately** checkbox.

Important: You might have to wait several minutes before your app becomes active.
 - d) To preview the contents of an app after it is added and before it is installed, select it from the list of extensions, and click **More Details**. Expand the folders to view the individual content items in each group.
3. Upgrade the UEBA app.
 - If the IBM QRadar Hub app is configured on QRadar, use the following instructions to install the UEBA app: [Downloading apps with the IBM QRadar Hub app](#).
 - If the IBM QRadar Hub is not configured, download the UEBA app archive from the [IBM Security App Exchange](#) onto your local computer. You must have an IBM ID to access the IBM Security App Exchange.
4. In the window that prompts you to update the current app version, leave the **Replace existing items** option selected and click **Install**. All of your existing app data remains intact.

Important: You might have to wait several minutes before your app becomes active. After the UEBA app is upgraded, the content packages are upgraded in the background. The content might not be visible in QRadar immediately after the app is upgraded.

Note: After the UEBA upgrade completes, content packages are upgraded automatically if the **Install and upgrade UBA content packages** setting is enabled on the “[Configuring content package settings](#)” on page 32 page. For more information about content packages, see “[UEBA content pack summary](#)” on page 83.

5. If the Machine Learning Analytics app is installed, the UEBA app automatically upgrades the ML app version.

What to do next

When the upgrade is complete, clear your browser cache and refresh the browser window before you use the app.

Related concepts

[“What's new in the QRadar User Entity Behavior Analytics app” on page 2](#)

Learn about the new features and enhancements in the latest QRadar User Entity Behavior Analytics (UEBA) app releases.

Chapter 4. Configuring the User Entity Behavior Analytics app

Before you can use the IBM QRadar User Entity Behavior Analytics (UEBA) app, you must configure additional settings.

You can import users directly into the UEBA app from an LDAP server, Active Directory server, CSV file, and reference table with the User import wizard. Note: Starting with UEBA 3.6.0, the LDAP app is no longer included with the UEBA app.

Complete the following setup procedures:

- Configure UEBA settings for the UEBA app
- Configure user imports

Configuring UEBA settings

To view information in the IBM QRadar User Entity Behavior Analytics (UEBA) app, you must configure UEBA application settings.

Configuring the authorization token in QRadar settings

To view information in the IBM QRadar User Entity Behavior Analytics (UEBA) app, you must configure a UEBA authorization token in UEBA Settings.

About this task

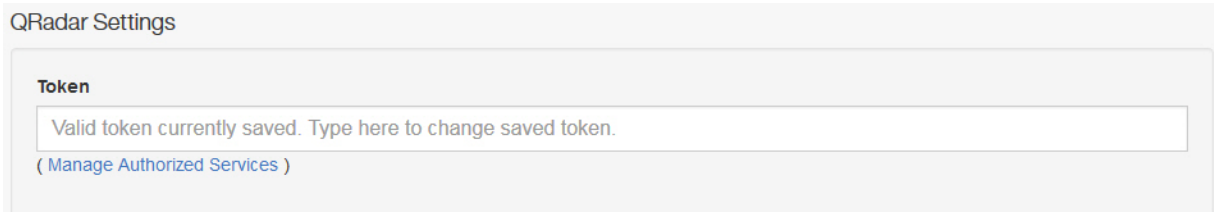
QRadar on Cloud administrators can learn how to add and manage authorized service tokens by reading https://www.ibm.com/support/knowledgecenter/SSKMKU/com.ibm.qradar.doc/c_qrocss_manageauthservices.html.

If you're a QRadar on Cloud customer, contact Customer Support to create an authorized service token for you.

You must complete the following steps to create an authorization token. Do not save the configuration until you have configured all of the UEBA Settings.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. Click the **UBA Settings** icon. (**Apps > User Entity Analytics > UBA Settings**).
3. In the QRadar Settings section, click the **Manage Authorized Services** link.



4. Click **Add Authorized Service**
5. In the **Service Name** field, type UBA.
6. From the **User Role** list, select the **Admin** user role.
7. From the **Security Profile** list, select the security profile that you want to assign to this authorized service. The security profile determines the networks and log sources that this service can access on the QRadar user interface.

8. In the **Expiry Date** list, type or select a date for this service to expire. If an expiry date is not necessary, select **No Expiry**.
9. Click **Create Service**.
10. Click the row that contains the UEBA service you created and then select and copy the token string from the **Selected Token** field in the menu bar.
11. Return to the **QRadar Settings** section and paste the authorized service token string into the **Token** field.

What to do next

[“Configuring content package settings” on page 32](#)

Configuring content package settings

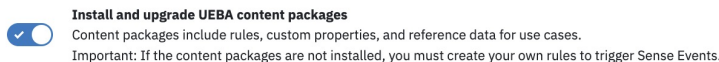
To view information in the IBM QRadar User Entity Behavior Analytics (UEBA) app, you must configure content package settings.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. Click the **UBA Settings** icon. (**Apps > User Entity Analytics > UBA Settings**).
3. In the Content Package Settings section, the **Install and upgrade UBA content packages** checkbox is enabled by default. If you do not want to install the UBA content packages, clear the checkbox and save the configuration. If you decide not to install UBA content packages, you must create your own rules to trigger sense events that send events to UEBA.

Note: If you clear the **Install and upgrade UBA content packages** checkbox and save the configuration and then return to the **UBA Settings** page and decide to select the checkbox and save the configuration, the content will be installed and upgraded.

Content Package Settings



What to do next

[“Configuring application settings” on page 32](#)

Configuring application settings

To view information in the IBM QRadar User Entity Behavior Analytics (UEBA) app, you must configure UEBA application settings.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. Click the **UBA Settings** icon. (**Apps > User Entity Analytics > UBA Settings**).
3. In the Application Settings section, configure the following settings:

Option	Description
Monitor imported users only	By selecting the Monitor imported users only setting, the UEBA app will not monitor new users that are discovered from events. UEBA will monitor only users that you imported.

Option	Description
User Risk threshold	<p>Indicates how high a user's risk score should get before an offense is triggered against that user. A <i>risk score</i> is the summation of all risk events that UEBA rules detect.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> • Dynamic: The default value is 4.0. The higher the value is, the higher the dynamic threshold will be, resulting in fewer offenses. Turn off Generate an offense for high risk users until the settings have run for at least a day. The dynamic threshold value is updated hourly based on risk score distribution in the system. You can determine whether you want to enable the setting based on the number of offenses that might be triggered. See the Tip for more information. <p>Note: If there is not enough variety in their scores, the risk score is set to +10 of the highest risk user. It stays that way to prevent many offenses from being generated unnecessarily.</p> <ul style="list-style-type: none"> • Static: The default value is 100,000. The value is set to a high value by default to avoid triggering offenses before the environment is analyzed. You can turn on Generate an offense for high risk users to open an offense with a username type for users above the risk threshold. You can determine whether you want to enable the setting based on the number of offenses that might be triggered. <p>Tip: Consider setting up UEBA and leaving the default value. Allow the settings to run for at least a day to see the type of scores that are returned. After a few days, review the results on the dashboard to determine a pattern. You can then adjust the threshold. For example, if you see one or two people with scores in the 500s but most are in the 100s then consider setting the threshold to 200 or 300. So "normal" for your environment might be 100 or so, and any score above that might require your attention.</p>
Entity Risk threshold	<p>Indicates how high an entity risk score should get before an offense is triggered against that entity. A <i>risk score</i> is the summation of all risk events that UEBA rules detect.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> • Dynamic: The default value is 4.0. The higher the value is, the higher the dynamic threshold will be, resulting in fewer offenses. Turn off Generate an offense for high risk users & entities until the settings have run for at least a day. The dynamic threshold value is updated hourly based on risk score distribution in the system. You can determine whether you want to enable the setting based on the number of offenses that might be triggered. See the Tip for more information. <p>Note: If there is not enough variety in their scores, the risk score is set to +10 of the highest risk user. It stays that way to prevent many offenses from being generated unnecessarily.</p> <ul style="list-style-type: none"> • Static: The default value is 100,000. The value is set to a high value by default to avoid triggering offenses before the environment is analyzed. <p>Tip: Consider setting up UEBA and leaving the default value. Allow the settings to run for at least a day to see the type of scores that are returned. After a few days, review the results on the dashboard to determine a pattern. You can then adjust the threshold. For example, if you see one or two people with scores in the 500s but most are in the 100s then consider setting the threshold to 200 or 300. So "normal" for your environment might be 100 or so, and any score above that might require your attention.</p>

Option	Description
Decay risk by this factor per hour	<p>Risk decay is the percentage that the risk score is reduced by every hour. The default value is 0.5.</p> <p>Tip: The higher the number, the faster the risk score decays; the lower the number, the slower the risk score decays. A value of zero will disable the feature.</p>
Date range for user detail graphs	<p>The date range that is displayed for the user details graphs on the User Details page. The default value is 1.</p>
Duration of investigation status	<p>The number of hours (1 - 10,000) that is assigned for an investigation to be completed.</p>
User inactivity interval	<p>The User Details page shows a timeline with activity grouped by sessions. If a user is inactive for the amount of time entered in the User inactivity interval field, the session ends. The default value is 15 minutes.</p>
Dormant account threshold	<p>The number of days that users are inactive before they are considered dormant. The default value is 14 days. For more information, see “Dormant accounts” on page 55.</p>
Maximum risk score	<p>Enter a value to set the limit for the maximum risk score on the Rules and Tuning page. Current risk scores are not affected by changes to this setting. Note: Rules that are delivered with the UEBA app typically have a risk score in the range of 5 - 25.</p>
Search assets for username, when username is not available for event or flow data	<p>Select the checkbox to search for user names in the asset table. The UEBA app uses assets to lookup a user for an IP address when no user is listed in an event.</p> <p>Important: This feature might cause performance issues in the UEBA app and your QRadar system.</p> <p>Important: Enabling the Search assets for username, when username is not available for event or flow data checkbox on the UBA Settings page can cause the User Details page to not load. Review the Rules pages to determine whether the enabled rules require this setting. It should be disabled if it is not needed.</p> <p>Tip: If the query timeout threshold is exceeded, the app does not return any data. If you receive an error message on the UEBA Dashboard, clear the checkbox and click Refresh.</p>
Display country/region flags for IP addresses	<p>Clear the checkbox if you do not want to display country and region flags for IP addresses.</p>
Monitored Entities	<p>Clear the checkbox if you do not want to monitor entities.</p>

Application User And Entity Settings

Monitor imported users only
Enabling this setting prevents UEBA from monitoring new users that are discovered from events.

User Risk threshold Static ▾
Static User risk threshold [≥ 1]
59 Value

Entity Risk threshold Static ▾
Static Entity risk threshold [≥ 1]
50 Value

Generate an offense for high risk users and entities
UEBA can open a username type and entity type offense for users and entities above the risk threshold.
The number of entity offenses that can be generated based on the threshold value you entered: 0.
The number of user offenses that can be generated based on the threshold value you entered: 0.

Decay risk by this factor per hour [0 - 0.99999]
0.5 Factor

Date range for user and entity detail graphs [1 - 7 Days]
1 Days

Duration of investigation status [1 - 10,000 Hours]
24 Hours

User And Entity inactivity interval [5 - 120 Minutes]
30 Minutes
Enter a duration in minutes that defines when a session ends. A session ends when there is no activity seen for the duration specified.

Dormant User accounts threshold [≥ 1 Days]
14 Days
Enter the number of days that users are inactive before they are considered dormant.

Search assets for username, when username is not available on event or flow data
Important: Required for flow-based rules. Enabling this setting can affect UEBA and QRadar performance.

Display country/region flags for IP addresses

Monitor Entities
Enabling this setting allows app to begin discovering and monitoring entities

What to do next

You can import users from the User import wizard. For more information, see [“Importing users” on page 35](#).

Configure user import

You can import users with the User Import wizard. The User Import wizard helps you to import users from an LDAP server, an Active Directory server, from reference tables, and CSV files directly into UEBA.

Tip: With the User Import wizard, you can import users and user data directly from within the UEBA app.

In 4.1.0 or later, you can create custom attributes with the User Import wizard.

Importing users

You can import users from within the UEBA app. The User Import wizard helps you to import users from an LDAP server, an Active Directory server, from reference tables, and CSV files.

Before you begin

You must configure the UEBA authorization token and admin permissions before adding import configurations. For more information, see [“Configuring the authorization token in QRadar settings” on page 31](#).

Important: The User Import wizard allows you to import users and user data directly from the UEBA app.

About this task

Note: The key names should always be in English. That means the attributes in reference tables and LDAP servers should also be in English.

You can access the **User imports** wizard from the following locations:

- The Admin Settings page (**Admin Settings > User Entity Analytics > User Import**).
- The **User Import** icon in the top menu bar on the UBA dashboard.
- The Import User Data section on the UEBA Settings page.

Procedure

1. On the **User Imports** window, click **Add**.
2. From the following options, select the source that you want to use to import user data:

- [LDAP/AD](#)
- [Reference Table](#)
- [CSV file](#)

3. After you add an import, you can view the status information for each configuration.

- Retrieval limit: The maximum number of users to poll per poll.
- Polling interval: The time in hours after the last successful poll.
- Last edited: The last time the configured changed.
- Users extracted: The total number of users in the current import configuration.

Note: The number of users extracted in each poll might be limited by a particular LDAP server. For example, when Paged results is not selected, an Active Director Server could only return up to 1000 records.

- Last poll date: The last time a poll was attempted.
- Last poll status: The status of the last poll (Failed, Idle, Warning, Running, Coalescing, Succeeded).

You can edit or delete the configuration. If you click the **Delete** icon you can select from the following options:

- Delete the configuration only. Any users or data that are imported from this configuration remains in UBA. This option removes the entry but does not remove the users from UEBA.
- Delete the configuration and users. Any users and their data will be removed from UEBA. This option removes both the configuration and users from UBA.
- Delete the configuration, users, reference table, and map of sets. You will only see this option if you selected the **Synchronize reference table** when you configured an LDAP/AD import. Note: Reference tables and map of sets will not be removed if they are used by any rule.

You can also select the **Import data now** icon to poll the server for data at any time.

Tip: To improve performance, you should delete import configurations that you no longer use.

What to do next

Configure the import from your LDAP/AD server, CSV file, or a reference table.

Related concepts

[How user imports in UEBA synchronizes imported data to a reference table](#)

Synchronizing imported data when you import users, causes some data to be stored and other data to be updated.

[“How user imports in UEBA synchronizes imported data to a reference table” on page 44](#)

Synchronizing imported data when you import users, causes some data to be stored and other data to be updated.

Related tasks

Importing users with LDAP or Active Directory

You can import user data, directly into the UEBA app, from an LDAP or Active Directory server.

Importing users from a reference table

You can import user data, directly into the UEBA app, from a reference table.

Importing users from a CSV file

You can import user data, directly into the UEBA app, from a CSV file.

Tuning user import configurations

After completing the import configurations, you can tune the configurations by selecting attributes to define valid usernames that combine users and enrich data that is displayed in UEBA by defining attributes for display data.

Importing users with LDAP or Active Directory

You can import user data, directly into the UEBA app, from an LDAP or Active Directory server.

Before you begin

You can import users with the User import wizard. For more information, see [“Importing users” on page 35](#)

About this task

Tip:

After an import is configured and the task has run to completion at least once, you should go to the Tuning page and make any necessary adjustments to the attributes.

Procedure

1. On the **User imports** window, click **Add** and then click **LDAP/AD**.
2. In the **Protocol** field, select **ldap://** or **ldaps://** for TLS.
3. In the **LDAP Server Host** field, enter an IP address or hostname. For example, 10.10.10.10 or sample.ldap.server.
4. In the **Port** field, enter the port for the LDAP server.
5. In the **Username (Bind DN)** field, enter the user name that is used to authenticate the LDAP server and enter the password in the **Password** field.
6. Click **Advanced Settings**. Note: You can change the **Base DN**; otherwise, when you click **Test Connection** the system determines the default values that are most applicable and populates the Base DN.
7. In the **Base DN** field, the field is auto-populated or you can enter the point in the LDAP directory tree from where the server must search for users. For example, if your LDAP server was on the domain example.com, you might use: dc=example, dc=com.
8. In the **Filter** field, enter the attribute or attributes you want to use to identify the users in a search request. For example: cn=*; uid=*; sn=*. The following default values will work with Active Directory: (&(sAMAccountName=*)(samAccountType=805306368)). For more information, see <https://ldap.com/ldap-filters/>.
9. In the **Certificate** field, click the **Upload** icon to add a root certificate authority (PEM) file.
10. The **Paged results** checkbox is selected by default to avoid limiting the number of records the LDAP server returns for each poll. Paged results are not supported by all LDAP servers.
11. Click **Test Connection** to confirm that UBA can connect to the LDAP server.
12. Click **Next**.

13. On the **Other import settings** screen, in the **Configuration name** field, enter a name to represent the configuration.
14. If you want to update the reference table with user imported data, enable **Synchronize reference table**. (Available in 3.8.0 and later.)
 - a) In the **Reference table name** field, enter a name.
 - b) In the **Reference table outer key** field, select a unique value to group all other attributes. Note: The outer key list is populated from the attributes list when you click **Test connection** on the **LDAP server configuration** page.
 - c) Select the **Generate map of sets** checkbox to make data available for use in rules and searches.
15. In the **Polling interval** field, define how often you want the app to poll your LDAP server for data. You can enter a polling interval of zero to manually poll. If you enter a polling interval of zero, you must poll the app manually with the poll option that is displayed in the feed.
16. In the **Retrieval limit** field, enter a value for the number of records you want the poll to return. The maximum number of records that can be returned is 500,000.
17. Click **Next** to review the summary of the configuration and then click **Save**.

What to do next

You can add more import configurations or continue tuning your existing import configurations.

Related concepts

[How user imports in UEBA synchronizes imported data to a reference table](#)

Synchronizing imported data when you import users, causes some data to be stored and other data to be updated.

[“How user imports in UEBA synchronizes imported data to a reference table” on page 44](#)

Synchronizing imported data when you import users, causes some data to be stored and other data to be updated.

Related tasks

[Importing users](#)

You can import users from within the UEBA app. The User Import wizard helps you to import users from an LDAP server, an Active Directory server, from reference tables, and CSV files.

[Importing users from a reference table](#)

You can import user data, directly into the UEBA app, from a reference table.

[Importing users from a CSV file](#)

You can import user data, directly into the UEBA app, from a CSV file.

[Tuning user import configurations](#)

After completing the import configurations, you can tune the configurations by selecting attributes to define valid usernames that combine users and enrich data that is displayed in UEBA by defining attributes for display data.

Importing users from a reference table

You can import user data, directly into the UEBA app, from a reference table.

Before you begin

You can access the User import wizard. For more information, see [“Importing users” on page 35](#)

About this task

You can import user data, directly into the UEBA app, from a reference table. For more information about reference data in QRadar, see [Using reference data in QRadar](#).

Procedure

1. On the **User Imports** window, click **Add** and then click **Reference table**.
2. From the **Reference table name** list, select a reference table.

Note: The fields will populate based on the information in the selected reference table.

Reference table configuration

Select a reference table from the list.

Reference table name

Number of entries in reference table: 82

Reference table attributes with samples

Attribute	Samples
accountExpires	9223372036854775807 more
adminCount	
badPasswordTime	131201481003349092 more
badPwdCount	4 more
codePage	

3. Click **Next**.
4. In the **Polling interval** field, define how often you want the app to poll for data from the reference table. You can enter a polling interval of zero to manually poll. If you enter a polling interval of zero, you must poll the app manually with the poll option that is displayed in the feed.
5. In the **Retrieval limit** field, enter a value for the number of records you want the poll to return. The maximum number of records that can be returned is 500,000.

Other import settings

Set the polling interval and the retrieval limit for polling data from reference table.

Polling interval *

Enter 0 for manual poll or set the polling interval with value between 8 and 8640.

Retrieval limit *

Enter an integer value between 1 and 500000.

6. Click **Next** to review the summary of the configuration and then click **Save**.

What to do next

You can add more import configurations or continue tuning your existing import configurations.

Related concepts

[How user imports in UEBA synchronizes imported data to a reference table](#)

Synchronizing imported data when you import users, causes some data to be stored and other data to be updated.

Related tasks

Importing users

You can import users from within the UEBA app. The User Import wizard helps you to import users from an LDAP server, an Active Directory server, from reference tables, and CSV files.

Importing users with LDAP or Active Directory

You can import user data, directly into the UEBA app, from an LDAP or Active Directory server.

Importing users from a CSV file

You can import user data, directly into the UEBA app, from a CSV file.

Tuning user import configurations

After completing the import configurations, you can tune the configurations by selecting attributes to define valid usernames that combine users and enrich data that is displayed in UEBA by defining attributes for display data.

Importing users from a CSV file

You can import user data, directly into the UEBA app, from a CSV file.

Before you begin

You can access the User import wizard. For more information, see [“Importing users” on page 35](#)

About this task

You can import user data, directly into the UEBA app, from a CSV file. The data is automatically loaded after you upload the file. You cannot reimport the same file and you cannot edit or repoll.

Procedure

1. On the **User Imports** window, click **Add** and then click **CSV File**.
2. Upload a CSV file. You can drag or click browse to open the file.
Important: The CSV file must be in UTF-8 format must not be greater than 10 MB. It must contain a header that has column names, use commas to delimit, and must contain at least one column with unique data.
3. Click **Next** to open the **Other import settings** screen.
4. If you want to update the reference table with user-imported data, enable **Synchronize reference table**. (Available in UEBA 3.8.0 and later.)
 - a) In the **Reference table name** field, enter a name.
 - b) In the **Reference table outer key** field, select a unique value to group all other attributes.
 - c) Select the **Generate map of sets** checkbox to make data available for use in rules and searches.
5. Click **Next** to review the summary of the configuration and then click **Save**.

What to do next

You can add more import configurations or continue tuning your existing import configurations.

Related concepts

How user imports in UEBA synchronizes imported data to a reference table

Synchronizing imported data when you import users, causes some data to be stored and other data to be updated.

[“How user imports in UEBA synchronizes imported data to a reference table” on page 44](#)

Synchronizing imported data when you import users, causes some data to be stored and other data to be updated.

Related tasks

Importing users

You can import users from within the UEBA app. The User Import wizard helps you to import users from an LDAP server, an Active Directory server, from reference tables, and CSV files.

Importing users with LDAP or Active Directory

You can import user data, directly into the UEBA app, from an LDAP or Active Directory server.

Importing users from a reference table

You can import user data, directly into the UEBA app, from a reference table.

Tuning user import configurations

After completing the import configurations, you can tune the configurations by selecting attributes to define valid usernames that combine users and enrich data that is displayed in UEBA by defining attributes for display data.

Tuning user import configurations

After completing the import configurations, you can tune the configurations by selecting attributes to define valid usernames that combine users and enrich data that is displayed in UEBA by defining attributes for display data.

Before you begin

You can access the User import wizard. For more information, see [“Importing users” on page 35](#).

Note: If you are connecting to an Active Directory, you do not have to configure the Tuning page. The default values for the tuning are optimized for Microsoft Active Directory.

About this task

All LDAP attributes on the remote LDAP server are saved. By saving the LDAP attributes, it is possible to use all the values in the LDAP schema, even in the case of attributes that are not uniform to every LDAP record.

Note: When you remove aliases or display fields they are removed from your import configurations and future import tasks. You must manually add them back if you removed them.

In UEBA 4.1.0 or later, you can create custom attributes.

Procedure

1. On the **User Imports** window, click **Tuning**.
2. In the User Coalescing section, click **Edit**.
3. On the **Edit: User Coalescing** pane, select at least one attribute from the current imports, which UEBA can use to identify and combine activity from the different user names of each user. You can also remove an alias to uncoalesce (separate combined users) that you have previously coalesced. When you remove an alias it then recoalesces. Note that when you delete an alias it takes effect only when the value of that alias is not shared with the deleted imports.

Note:

Attributes added in the user coalescing section should be unique to an individual. Attributes that contain user names for various accounts used throughout the enterprise should be selected, such as 'samaccountname' or 'distinguished name'. Selecting values that are shared among many users, results in UEBA combining the users together. Values such as "department" and "country" should not be selected.

4. In the Display Fields section, click **Edit** to customize the attributes that you want to display on the **User Details** page. You can also click **Add** to select attributes for the selected display field.

Note:

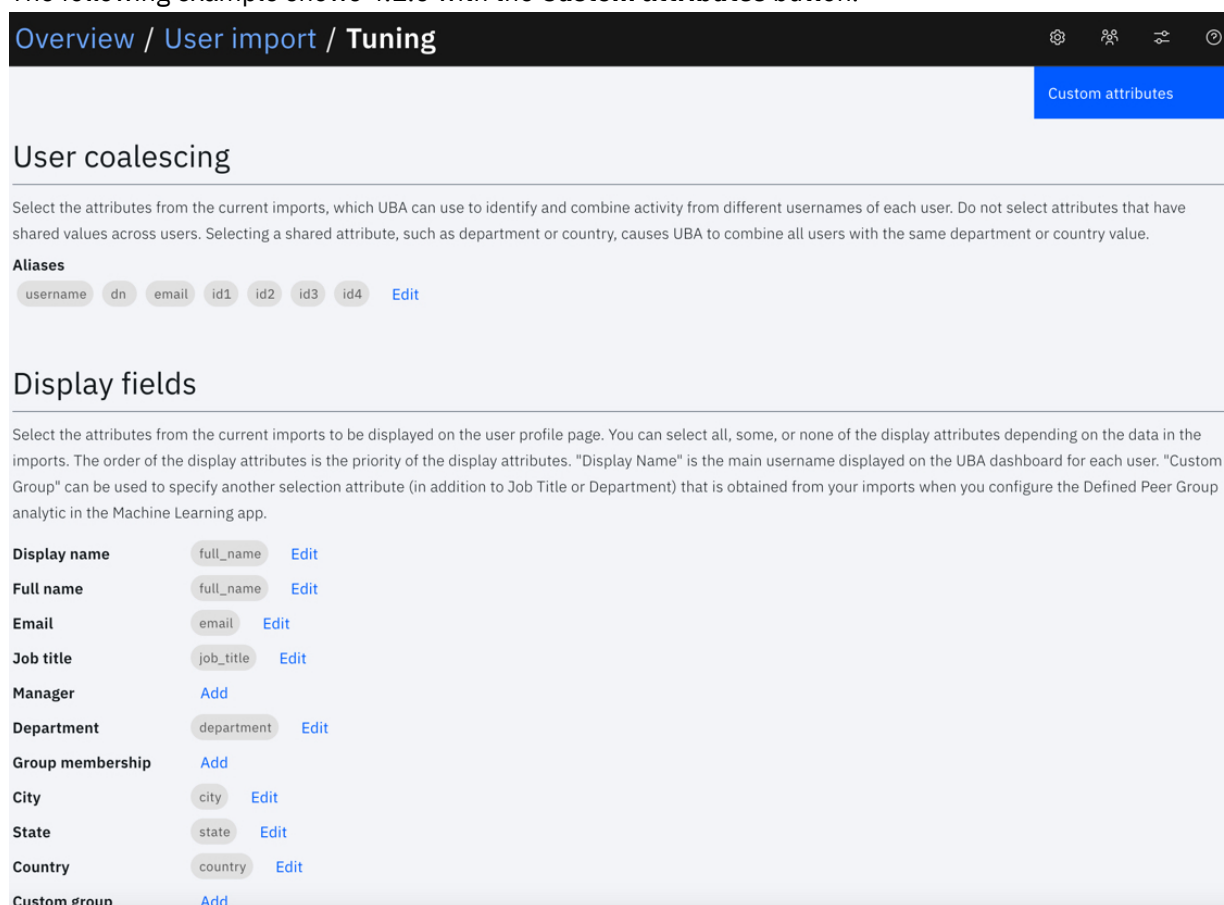
The order that the attributes are shown, determines the order that UEBA gets the value for the attributes to be displayed on the User Details page. For example, if the order of the attributes is "displayname" followed by "cn", then when user coalescing, if "displayname" has a value for that user, that value is used, and will not find the value of "cn". If "displayname" has no value, it will go to find the next attributes for "cn". If "cn" has no value, it will go to find the next attribute and so on.

Important: The **Custom group** display attribute is a special attribute that is used to define a grouping attribute that can be selected as the grouping mechanism for the Defined Peer Group Machine Learning analytic. This attribute is not displayed on the user profile page like the other display attributes. An attribute from the configured LDAP, reference table, or CSV file user import can be selected. The selected attribute should be one that allows for clustering of the user population. Examples of Active Directory attributes that might be useful for such grouping are "physicalDeliveryOfficeName", "memberOf" and "divison". Attributes that are unique per individual should not be selected. Do not use Custom group for any other purposes.

5. Click **Save**.

Note: After you click Save, the data that is imported from all sources is reprocessed based on the new selections of coalescing aliases and display keys.

The following example shows 4.1.0 with the **Custom attributes** button.



Results

Tip:

If you chose the wrong attribute for user coalescing and encounter issues, you can remove it and it will uncoalesce the attribute.

Related concepts

[How user imports in UEBA synchronizes imported data to a reference table](#)

Synchronizing imported data when you import users, causes some data to be stored and other data to be updated.

Related tasks

Importing users

You can import users from within the UEBA app. The User Import wizard helps you to import users from an LDAP server, an Active Directory server, from reference tables, and CSV files.

Importing users with LDAP or Active Directory

You can import user data, directly into the UEBA app, from an LDAP or Active Directory server.

Importing users from a reference table

You can import user data, directly into the UEBA app, from a reference table.

Importing users from a CSV file

You can import user data, directly into the UEBA app, from a CSV file.

Creating custom attributes

About this task

You can create custom attributes by combining existing attributes so that you can select them for coalescing and display fields from the Tuning page. You can search for custom attributes by name, formula, or sample.

Procedure

1. From the Tuning page, click **Custom attributes**.
2. Click **Add new**.
3. In the **Attribute Name** field, enter a name that you want to see on the Tuning page.
4. In the **Formula** field, enter the combination of attributes by starting with curly brackets. Tip: You can select from the list that populates, based on your existing data, to help build your formula.
In the Samples column, a sample of the data is auto-generated based on the formula that you created for that custom attribute.
5. You can click **Add new** to continue adding more custom attributes.
6. Click **Save**.

Results

The custom attributes you created are now available as selections when you click **Edit** next to Aliases and Display field.

Example



The following example shows 4.1.0 of the Custom attributes feature.

Custom attributes

Create custom attributes by combining existing attributes that can be selected on the Edit panel from the tuning page.

Note: Combining imported attributes can take several hours depending on the number of users. The selected aliases or display fields will display on the profile page when coalescing is complete.

Search for custom attributes Add new

Attribute Name ⓘ	Formula ⓘ	Samples	
attr	{department}{full_name}	Marketingtestuser_117947	
newtest	{domain}{city}{	a.testLondon{	

Number of rows: 2

department
 full_name
 id2
 ...

Cancel
Save

How user imports in UEBA synchronizes imported data to a reference table

Synchronizing imported data when you import users, causes some data to be stored and other data to be updated.

When each user import has completed the step to download data from the defined source (LDAP, reference table, or CSV file), UEBA searches the data that was retrieved from the source and parse it through a normalization process, which takes each record that is received and maps attributes from the source to a set of normalized fields. The fields are display_name, full_name, city, state, country, custom_group, dept, domain, email, job_title, manager. These fields are normalized as configured from the **User Imports > Tuning** tab in the display fields section.

If a display field has multiple attributes listed, the first attribute in the list is used to populate the normalized field in the reference table. Should an attribute from the import source contain a list of values, then the first value in the list will be used to populate the normalized field in the reference table. For example, if the display field 'Department' is configured to be set from imported attribute 'dept' and 'section' in that order, then the value for 'dept' will be stored in the reference table. Continuing the previous example, if 'dept' contained values 'Engineering' and 'Devops' in that order, then 'Engineering' will be stored in the reference table under the 'department' normalized field. Similarly, the user coalescing fields that are defined for the aliases section in the user import tuning page will be used to map each 'username' found to id, id1, id2, etc., up to the number of attributes in the aliases list. If no aliases are matched from the imported data, the user is not added to the reference table.

On initial run, or when the option to synchronize the data is added to an existing configuration, all values found by that import (and only that import) are added, the users are not coalesced and will not look like the users in UEBA exactly. If the import configured supports additional polling (like LDAP) then on each delta poll only the newly discovered records are added. UEBA will never completely rebuild the reference table from data. Therefore, if elements in the reference table are manually removed, they will not be automatically added back.

Related tasks

Importing users

You can import users from within the UEBA app. The User Import wizard helps you to import users from an LDAP server, an Active Directory server, from reference tables, and CSV files.

Importing users with LDAP or Active Directory

You can import user data, directly into the UEBA app, from an LDAP or Active Directory server.

Importing users from a reference table

You can import user data, directly into the UEBA app, from a reference table.

Importing users from a CSV file

You can import user data, directly into the UEBA app, from a CSV file.

Tuning user import configurations

After completing the import configurations, you can tune the configurations by selecting attributes to define valid usernames that combine users and enrich data that is displayed in UEBA by defining attributes for display data.

Chapter 5. Administering

Administrative functions

The QRadar User Entity Behavior Analytics (UEBA) app includes administrative functions for clearing UEBA data, removing event users, and resetting ML settings from the **Help and Support** page.

You must have QRadar administrator privileges to complete administrative functions.

You can access the **Help and Support** page from the following locations:

- From the Admin Settings, click **Apps > User Entity Analytics > Help and Support**.
- From the **User Entity Analytics** tab, click the **Help and Support** icon.

Clear UEBA Data

Click **Clear UBA Data** to remove all UEBA user data but maintain all of your current UEBA configuration settings. Clearing UEBA data makes the UEBA app behave as if you just installed and configured the **UBA Settings**. If the Machine Learning app is installed, the **Clear UBA Data** button also resets the ML app.

Remove event users

Click **Remove event users** to remove users that were discovered through events. You can click the number link to go to the search page that shows the list of users that will be deleted. After confirming the user removal, the count on the overview page under Users discovered from events should decrease to zero. Users that were imported are not affected and will not be removed. Tip: You should enable the **Monitor imported users only** option on the UEBA **Settings** page before removing event users if you don't want to discover users from events again. Note: If there are no event users, this option will be hidden.

Reset ML Settings

Click **Reset ML Settings** if the Machine Learning app is installed and you want to reset all of your Machine Learning settings and disable all of the analytics that are enabled.

Assigning user capabilities for the QRadar User Entity Behavior Analytics app

Administrators use the User Role Management feature in IBM QRadar to configure and manage user accounts. As an administrator, you must enable the User Entity Analytics, Offenses, and Log Activity permissions for each user role that is permitted to use the QRadar User Entity Behavior Analytics (UEBA) app.

About this task

After you install UEBA, it is displayed as a capability in **User Roles** on the **Admin** tab. To use the app, a QRadar administrator must assign the app, and any other capabilities that it requires, to a user role.

Security profiles are different than user roles. Security profiles define which networks, log sources, and domains that a user can access. For more information, see the Security Profiles section in the *IBM QRadar Administration Guide*. Security profiles or user roles that are overly restrictive can result in data not appearing.

Note: If you are deploying UEBA for use in a multitenant environment, see [“UEBA user roles for multitenancy”](#) on page 78.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the System Configuration section, click **User Management**, and then click the **User Roles** icon.
3. Select an existing user role or create a new role.
4. Select the following checkboxes to add the permissions to the role.
 - **User Entity Analytics**
 - **Offenses**
 - **Log Activity**
5. Click **Save**.

Creating watchlists

You can add and configure watchlists that include user-based members, entity-based members, and hybrid watchlists that combine both user and entity memberships.

About this task

You can add a user, entity, and hybrid to a new watchlist or an existing watchlist from the main UEBA Overview (Dashboard) page, the **User or Entity Details** page, or the **Search Results** page. A single user or entity can be a member of multiple watchlists. If a user creates a User watchlist, it contains only users. If an Entity watchlist is created, only entities can be added to it. You can add both users and entities in a Hybrid watchlist.

Procedure

1. From the main UEBA Overview (Dashboard) page or the **User Details** page, click the **Watchlist** icon.
2. From the menu, select **Create new watchlist**. To add a user to an existing watchlist, click **Add to** your watchlist.
3. On the **General Settings** tab, enter a watchlist name.
Select one of the Watchlist options:
 - User - Select this option to create a watchlist for users.
 - Entity - Select this option to create a watchlist for entities.
 - Hybrid - Select this option to create a combined watchlist for both users and entities.
4. Set the user's risk score by changing the value in the **User Scale risk by factor** field. If you select the default factor of '1', the risk score is unchanged.
5. Set the entity's risk score by changing the value in the **Entity Scale risk by factor** field. If you select the default factor of '1', the risk score is unchanged.
6. In the **Machine Learning tracking priority** section, select the priority for how users are tracked by the Machine Learning analytics.
 - High - Users are always tracked up to the maximum users per Machine Learning analytic.
 - Normal - Users are tracked by highest risk after all the high users are included.
 - Never - Users are not tracked by Machine Learning.
7. Set the **Refresh interval** (in hours) to control how often the watchlist membership updates. A value of zero means disable or manual refresh only.

Note: A hybrid watchlist can simultaneously include users and entities.

The following example shows Watchlist settings.

Create a watchlist

General settings User Membership settings Entity Membership settings

User
Entity
✓ Hybrid

Name

Enter a watchlist name

User Scale risk by factor
Enter a value in scale factor (0 - 10) to increase or decrease the user's risk.
For example, if you want to scale down your admin account, set the factor to '0.1'.

1 - +

Entity Scale risk by factor
Enter a value in scale factor (0 - 10) to increase or decrease the entity's risk.
For example, if you want to scale down your admin account, set the factor to '0.1'.

1 - +

Machine learning tracking priority
Select the priority for how users are added to machine learning.

High Normal Never

Cancel Next



8. On the **User Membership settings** tab, configure how members are determined:
 - a) In the **Import from QRadar reference set** field, search for a reference set or click to select a reference set from the list to import all entries from the reference set. After you select a reference set, click the link to review.

Note: The list might contain reference sets that do not have usernames.

Edit a watchlist

General settings

User Membership settings

Optional: You can import users with a reference set or regular expression or both.

Note: You can also add any user to a watchlist by clicking the Watchlist icon.

Import from QRadar reference set

Search for or select a reference set from your QRadar system.

UBA : Dormant Accounts

0 entries in QRadar

Add from monitored users with regex filter

Select a user property and enter a valid POSIX regular expression. The expression is case-sensitive.

For example, to retrieve all users with engineers in their job title select 'Job title' and enter '!*Engineer.*'.

You can also enter the '^\$' regular expression to match a missing property. For example, to find service accounts without an email address, select the property 'email' and enter '^\$'.

Select a property

[a-z]+

Cancel

Save

- b) In the **Add from monitored users with regex filter** field, you can select a user property and enter a valid POSIX regular expression to select users who are already found in the UEBA database. A count of matching users is displayed next to each regex filter to help administrators see the scope of the filter in real-time.

Create a watchlist

General settings

User Membership settings

Entity Membership settings

Optional: You can import entities with a reference set or regular expression or both.

Note: You can also add any entity to a watchlist by clicking the Watchlist icon.

Import from QRadar reference set

Search for or select a reference set from your QRadar system.

Add from monitored entities with regex filter

Select an entity property and enter a valid POSIX regular expression. The expression is case-sensitive.

For example, to retrieve all entities with 'hostname' contains '*abcd*'.

You can also enter the '^\$' regular expression to match a missing property. For example, to find service accounts without email address, select the property 'email' and enter '^\$'.

✓ Select a property

IP Address

Hostname

Linked Users

[a-z]+

Cancel Save

9. On the **Entity Membership settings** tab, configure how members are determined:
 - a) In the **Import from QRadar reference set** field, search for a reference set or click to select a reference set from the list to import all entries from the reference set. After you select a reference set, click the link to review.

Note: The list might contain reference sets that do not have usernames.
 - b) In the **Add from monitored users with regex filter** field, you can select regex on entity properties (Forex ample: IP address, hostname, Linked Users) to dynamically populate the watchlist. A count of matching users is displayed next to each regex filter to help administrators see the scope of the filter in real-time. If you select **IP Address** (CIDR range), you can choose from a list of CIDR ranges that are already available within the system. These predefined IP ranges can be selected as needed.
10. After configuring membership settings, click **Save**.

11. Go to the UEBA dashboard to view entities that have been added to a watchlist. Review the displayed entities, which are automatically refreshed based on the **Refresh interval** configured in the watchlist settings.

Note: The UEBA dashboard displays only a limited number of entities.

12. To view all entities associated with the watchlist, click **View all entities** on the dashboard. The system navigates to the **Watchlist** page, where the complete list of entities is displayed.

The screenshot shows a dashboard titled "h-1" with a tab for "Entities (1)". Below the tab is a table with the following columns: "IP and Host", "Linked Users", "Recent risk", and "Overall risk". The table contains one row with the following data:

IP and Host	Linked Users	Recent risk	Overall risk
192.168.184.213	local_to_...	0	10.93

At the bottom right of the dashboard, there is a link that says "View all 1 entities" with a list icon.

Viewing the trusted users list

You can view the list of trusted users in the reference set management list.

Procedure

1. On the navigation menu (☰), click **Admin**.

2. In the System Configuration section, click **Reference Set Management**.
3. On the **Reference Set Management** window, select the **UBA : Trusted Usernames** reference set.
4. Click **View Contents**.

Managing network monitoring tools

You can manage network monitoring tools for the IBM QRadar User Entity Behavior Analytics (UEBA) app.

About this task

If you want to monitor the use of network capture, monitoring or analysis program usage, make sure the programs are listed in the UBA : Network Capture, Monitoring and Analysis Program Filenames reference set. You must then enable the **UBA : Network Capture, Monitoring and Analysis Program Filenames** rule.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the System Configuration section, click **Reference Set Management**.
3. On the **Reference Set Management** window, select the **UBA : Network Capture, Monitoring and Analysis Program Filenames** reference set.
4. Click **View Contents**.
5. To add an application to manage, click **Add** and enter the values in the box.
6. To remove an application, select an application and click **Delete**.

What to do next

Enable the **UBA : Network Capture, Monitoring and Analysis Program Filenames** rule.

Managing restricted programs

You can manage restricted programs for the IBM QRadar User Entity Behavior Analytics (UEBA) app.

About this task

If there are any applications that you want to monitor for usage, go to the UBA : Restricted Program Filenames reference set and enter the applications that you want to monitor. You must then enable the UBA : Restricted Program Filenames rule.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the System Configuration section, click **Reference Set Management**.
3. On the **Reference Set Management** window, select the **UBA : Restricted Program Filenames** reference set.
4. Click **View Contents**.
5. To add an application to manage, click **Add** and enter the values in the box.
6. To remove an application, select an application and click **Delete**.

What to do next

Enable the **UBA : Restricted Program Filenames** rule.

Adding log sources to the trusted log source group

If you do not want the IBM QRadar User Entity Behavior Analytics (UEBA) app to monitor and report certain log sources, you can add them to the **UBA : Trusted Log Source Group**. Adding log sources to the group stops the UBA app from monitoring them.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. Click the **Log Sources** icon.
3. Click **Add**.
4. Configure the common parameters for your log source.
5. Configure the protocol-specific parameters for your log source.
6. Select the **UBA : Trusted Log Source Group** checkbox.
7. Click **Save**.
8. On the **Admin** tab, click **Deploy Changes**.

New accounts

A user can have several accounts (aliases) associated to them. This association is achieved by configuring coalescing when you tune your Import Configurations for User Imports. Accounts that are owned by a user are added to UEBA by using three methods:

- Importing attributes from an LDAP source.
- Adding users from a QRadar reference set from a watchlist that is created within UEBA.
- Discovering users from a sense event. This can be limited to the first two methods by setting the **Monitor imported users only** in the Application settings section on UEBA Settings page.

An account added to UEBA from LDAP or watchlist will not have a score until they are seen on any event consumed by QRadar. An account added from a sense event will have a score, immediately, from the sense event that detected it.

Responses to new accounts

New accounts are set to active after being seen on an event. For more information on account status, see [Dormant Accounts](#). The "UBA : New Account Use Detected" rule is also triggered by the one-time event sent by the app. Custom responses can be created by using the event: "New Account Use Detected (QID 104000014)".

Related concepts

[“Configure user import” on page 35](#)

You can import users with the User Import wizard. The User Import wizard helps you to import users from an LDAP server, an Active Directory server, from reference tables, and CSV files directly into UEBA.

Related tasks

[“Tuning user import configurations” on page 41](#)

After completing the import configurations, you can tune the configurations by selecting attributes to define valid usernames that combine users and enrich data that is displayed in UEBA by defining attributes for display data.

[“Configuring application settings” on page 32](#)

To view information in the IBM QRadar User Entity Behavior Analytics (UEBA) app, you must configure UEBA application settings.

Dormant accounts

You can see users in your system that have dormant accounts, active accounts, or accounts that have never been used.

Viewing dormant accounts on the User Details page

You can see the status of the accounts that are associated with the selected user on the User Details page.

User Account Status	Description
Active	An account that UEBA has seen events from a QRadar log source within the configured dormant account threshold time period.
Dormant	An account that UEBA has seen at least one event from in the past but has not seen any new events during the dormant account threshold time period.
Never Used	<p>An account for which UEBA has never seen an event with that user name in a QRadar log source.</p> <p>Accounts identified as "Never Used" can be caused by the following activities:</p> <ul style="list-style-type: none"> Accounts that have never been logged by a QRadar log source for the associated user name account. The event occurred before UEBA 3.2.0 was installed. Note: When you first install the UEBA app, only events that occurred in the last hour are analyzed to determine when an account was last accessed. After the initial analysis, the UEBA app queries events that occurred between executions of the background task that watches for account usage. <p>Note: Accounts that are categorized as "Never Used" were likely imported from the LDAP app.</p>

Test User 1

Web Developer
Development
Dallas, TX, US

Overall Risk Score **5K** ↗

Risk last Interval **1K**

Active	testuser1
Dormant ⚠	testuser1_admin
Never Used	testuser1_db
	testuser1@exam...

Users with Dormant Accounts watchlist

The Users with Dormant Accounts watchlist is automatically generated as the UEBA app pulls in user data. You can view the Users with Dormant Accounts watchlist on the UEBA Dashboard.

If you delete the watchlist, it is not automatically re-created. If you need to create it again, select the **UBA : Dormant Accounts** reference set on the **Membership Settings** tab on the Create a watchlist screen.

Configuring the dormant accounts threshold

The default value for the dormant accounts threshold is 14 days. You can change the number of days that users are inactive before they are considered dormant in the Application Settings section on the UEBA Settings page (**Admin Settings > User Entity Analytics > UBA Settings**).

Responses to dormant accounts or users

You can generate responses for dormant accounts from the provided rules. You can also create custom responses by using the events that are triggered from the app.

To use the provided rules so that a user's score is increased when an account that was dormant is used or is attempted to be used, make sure that the following rules are enabled:

- [“UEBA : Dormant Account Use Attempted” on page 119](#)
- [“UEBA : Dormant Account Used” on page 118](#)

To create custom responses, you can use the following generated events in a rule or query:

- Dormant Account Found (QID 104000012)
- Dormant Account Used (QID 104000013)

Related concepts

[“UEBA overview and user details” on page 17](#)

The IBM QRadar User Entity Behavior Analytics (UEBA) app shows you the overall risk data for users in your network.

Related tasks

[“Configuring application settings” on page 32](#)

To view information in the IBM QRadar User Entity Behavior Analytics (UEBA) app, you must configure UEBA application settings.

[“Creating watchlists” on page 48](#)

You can add and configure watchlists that include user-based members, entity-based members, and hybrid watchlists that combine both user and entity memberships.

Resetting machine learning model


The Reset Model feature enables security teams to restart individual machine learning models from a clean baseline while preserving all custom configurations. This process removes previously learned behavioral data, allowing the model to retrain by using current and accurate information without impacting existing system settings or ongoing operations.

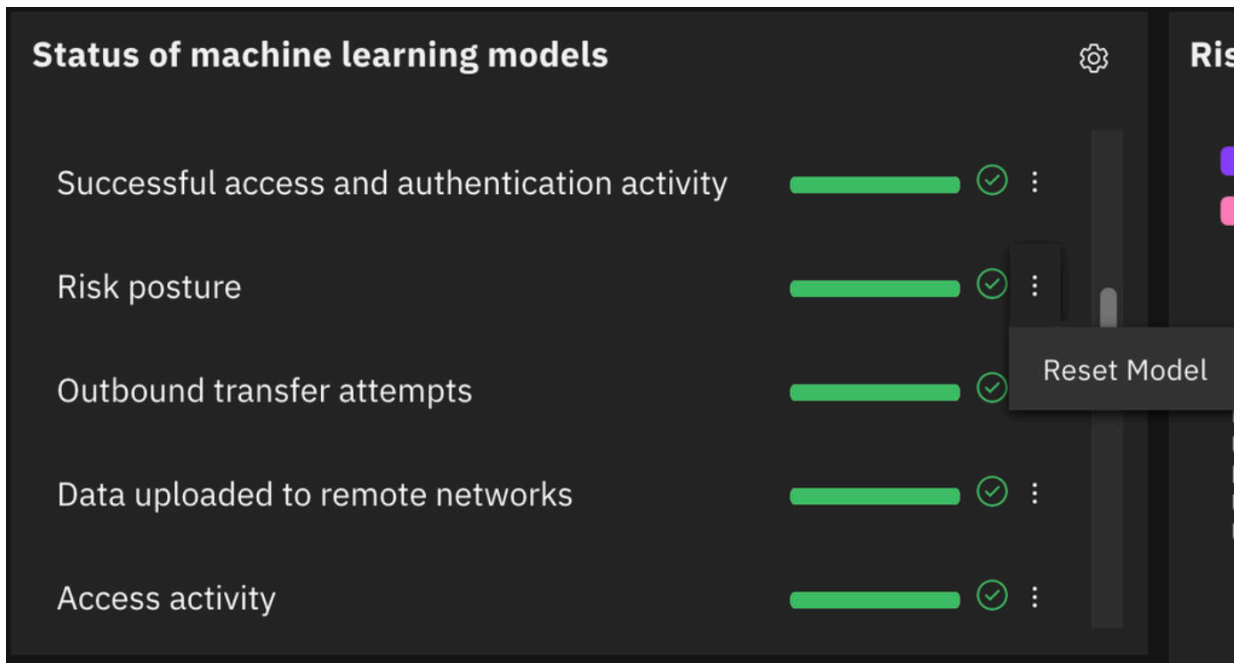
About this task

The Reset Model feature is used in the following scenarios:

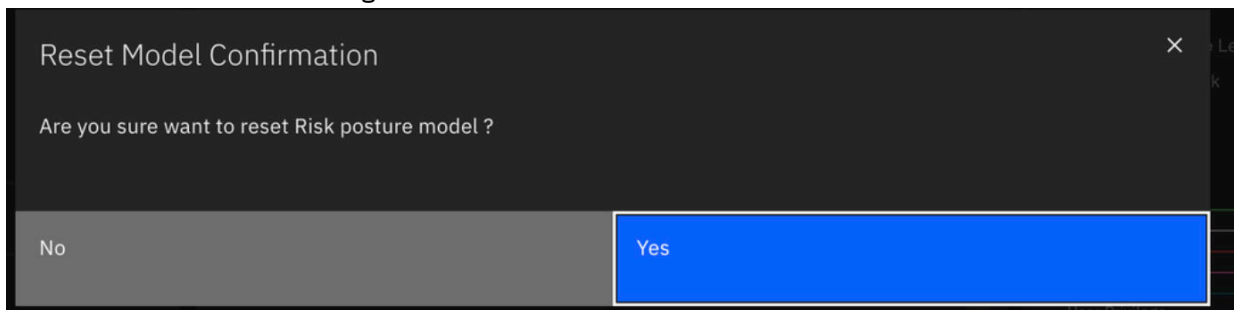
- Resolving issues caused by inaccurate, incomplete, or corrupted historical training data.
- Enabling rapid model adaptation to significant organizational changes, such as mergers, acquisitions, or structural reorganization.
- Improving detection accuracy when model performance degrades, including increased false positives or missed threat activity.
- Supporting compliance and regulatory requirements that mandate periodic model retraining or refresh cycles.

Procedure

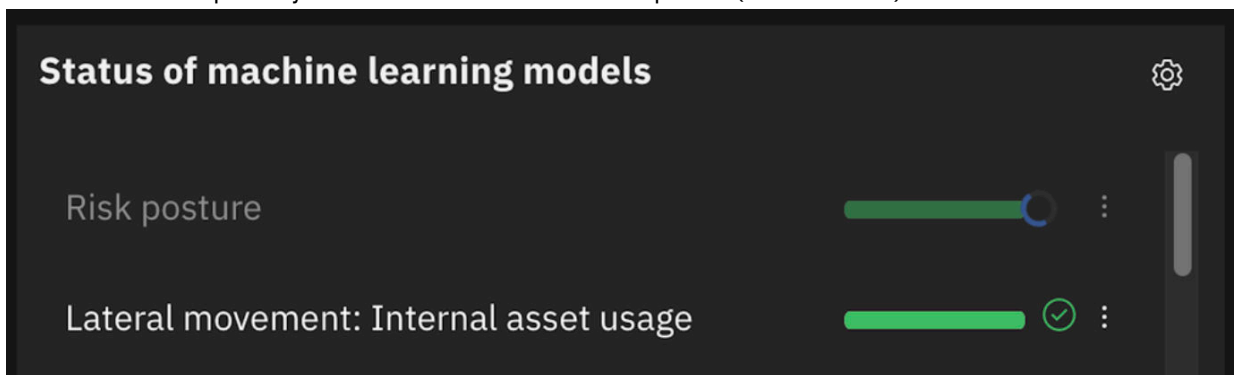
1. Go to the UEBA dashboard and select the machine learning model that you want to reset.
2. Click () menu next to the selected machine learning model and select **Reset Model**.



3. Review the confirmation dialog and click **Yes**.



The model is temporarily disabled while the reset completes (1–5 minutes).



Active investigation in User Entity Behavior Analytics app

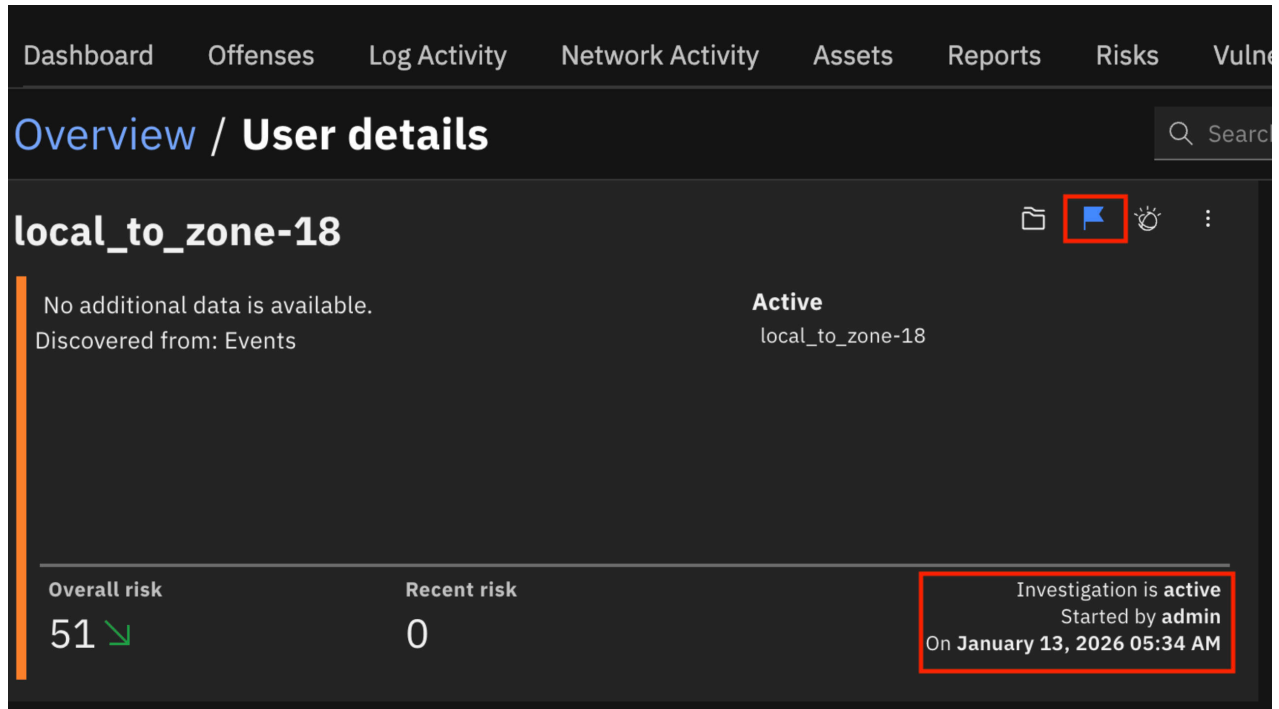
An Active Investigation identifies a user or entity under review for potential security risks and records the initiator along with the start date and time.

Starting an investigation

1. From the dashboard, click a user name or the entity name. You can also search for a specific user or entity.
2. Locate the flag icon in the action bar.

3. Verify the investigation status. An outlined (empty) **flag** indicates that no active investigation currently exists.
4. Click the outlined **flag** icon to initiate an investigation.
5. Confirm that the icon changes to a filled (solid) **flag**, indicating the investigation is now active.
6. Review the **Investigation Status** banner, which appears and displays your user details along with the investigation start date and time.

Note: The process is identical for both users and entities.



Viewing an active investigation


You can view the **Active investigation** page by using one of the following procedures:


Dashboard widget (quick view)

The **Active investigations** card is on the main dashboard page. It displays two tabs: **User** and **Entity**, each showing up to ten active investigations. For each user or entity, the card presents the name, the current risk score along with a trend indicator, and the name of the individual conducting the investigation. A **View All** link is displayed on the card, which also indicates the total number of active investigations available for each tab.

Active investigations

My investigations

User (1)	Entity (2)
 local_to_zone-...	investigated by admin

[View all 1 users](#) 

Active investigation page (full view)

The **Active investigation** page is a dedicated page that is accessible from the dashboard widget. Users can access this page by clicking **View All Users** or **View All Entities** within the dashboard widget, or by going directly to the **Active investigation** page from the main menu.





IBM QRadar

Dashboard Offenses Log Activity Network Activity Assets Reports Risks Vulnerabilities Admin Pre-Validation **User Entity Analytics** System Time: 05:33

Overview / **Active investigations**

Active investigations My investigations

Users **Entities**

Entity	Investigated By	Recent risk	Overall risk	Start Time	End Time
 192.168.184.218	admin	10	30 	Jan 13 5:32 AM	Jan 14 5:32 AM
 192.168.172.235	admin	0	0 	Jan 12 3:54 PM	Jan 13 3:54 PM

Items per page 15 1-2 of 2 entities 1 1 of 1 page

Chapter 6. Tuning

Enabling indexes to improve performance

To improve the performance of your IBM QRadar User Entity Behavior Analytics (UEBA) app, enable indexes in IBM QRadar.

About this task

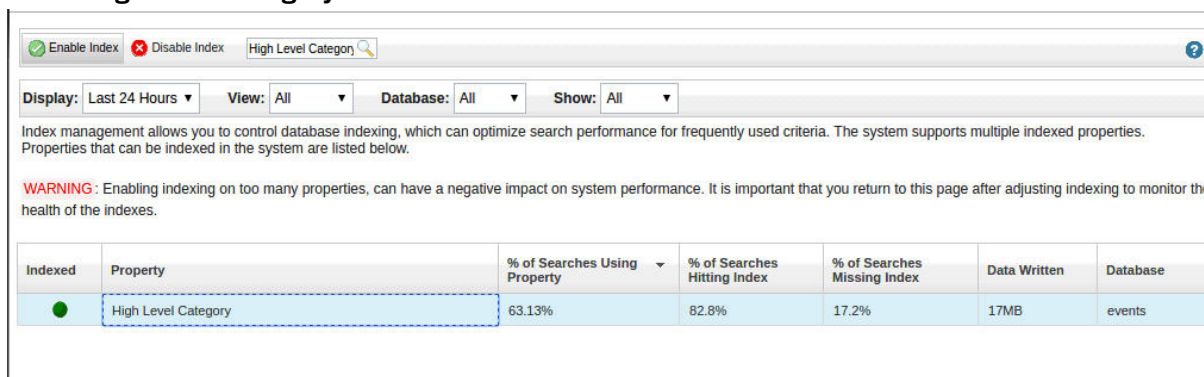
To improve the speed of searches in IBM QRadar and the UEBA app, narrow the overall data by adding the following indexed fields to your search query:

- High Level Category
- Low Level Category
- senseValue
- senseOverallScore
- Username

For more information about indexing, see [Index management](#).

Procedure

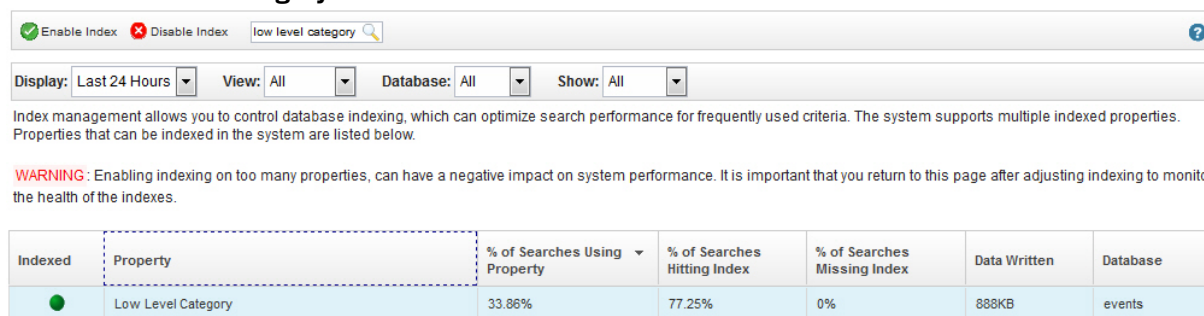
1. On the navigation menu (☰), click **Admin**.
2. In the System Configuration section, click the **Index Management** icon.
3. On the Index Management page, in the search box, enter High Level Category.
4. Select **High Level Category** and then click **Enable Index**.



The screenshot shows the Index Management interface. At the top, there are buttons for 'Enable Index' (with a green checkmark) and 'Disable Index' (with a red X), and a search box containing 'High Level Category'. Below these are filters for 'Display: Last 24 Hours', 'View: All', 'Database: All', and 'Show: All'. A paragraph explains that index management allows controlling database indexing to optimize search performance. A warning states: 'WARNING: Enabling indexing on too many properties, can have a negative impact on system performance. It is important that you return to this page after adjusting indexing to monitor the health of the indexes.' Below this is a table with the following data:

Indexed	Property	% of Searches Using Property	% of Searches Hitting Index	% of Searches Missing Index	Data Written	Database
●	High Level Category	63.13%	82.8%	17.2%	17MB	events

5. Click **Save**.
6. Select **Low Level Category** and then click **Enable Index**.



The screenshot shows the Index Management interface with the search box containing 'low level category'. The table below shows the following data:

Indexed	Property	% of Searches Using Property	% of Searches Hitting Index	% of Searches Missing Index	Data Written	Database
●	Low Level Category	33.86%	77.25%	0%	888KB	events

7. Click **Save**.
8. On the Index Management page, in the search box, enter sense.

9. Select **senseValue** and **senseOverallScore** and then click **Enable Index**.

The screenshot shows the Index Management interface. At the top, there are buttons for 'Enable Index' (checked) and 'Disable Index'. A search box contains 'sense'. Below this are filters for 'Display: Last 24 Hours', 'View: All', 'Database: All', and 'Show: All'. A paragraph explains that index management allows control over database indexing to optimize search performance. A warning states that enabling indexing on too many properties can negatively impact system performance. Below the text is a table with the following data:

Indexed	Property	% of Searches Using Property	% of Searches Hitting Index	% of Searches Missing Index	Data Written	Database
●	senseValue (custom)	11.5%	0%	100%	0KB	events
●	senseOverallScore (custom)	0.06%	0%	100%	0KB	events
	senseOffenseld (custom)	0%	0%	0%	0KB	events
	senseOffenseScore (custom)	0%	0%	0%	0KB	events
	senseWindowScore (custom)	0%	0%	0%	0KB	events

10. Click **Save**.

11. On the Index Management page, in the search box, enter **username**.

12. Select **Username** and then click **Enable Index**.

The screenshot shows the Index Management interface with 'username' in the search box. The table below shows the following data:

Indexed	Property	% of Searches Using Property	% of Searches Hitting Index	% of Searches Missing Index	Data Written	Database
●	Username	10.12%	99.45%	0%	22MB	events
	Identity Username	0%	0%	0%	0KB	events

13. Click **Save**.

Integrating new or existing QRadar content with the UEBA app

To meet your specific needs, you can use the capabilities that are built into QRadar by integrating your existing QRadar rules with the UEBA app.

Before you begin

The following lists the three types of content that work with UEBA:

- Content that is created by UEBA and installed with a risk score.
- Content that is not created by UEBA but has a risk score and works with UEBA by default. For more information, see [“Supported QRadar content”](#) on page 232.
- All other content in QRadar that can be modified to work with UEBA.

UEBA uses a QRadar reference table ("UBA: Rule Data") to determine the score to give the events that are sent by the rules that work with UEBA. When UEBA is installed, the table is initially populated with all content that works with UEBA by default. A task runs every hour that pulls any rules that have been modified to include a sense value in the description into the Rule Data table.

Restriction: The sense value in the event description should not be modified. The risk score should be modified in either the UEBA Rules and Tuning page or the QRadar Use Case Manager.

Note: When rules are added to the reference table, they cannot be removed. To stop the rules from sending a risk score to UEBA, you can either disable the rule or set the risk score to zero. For more information, see [Chapter 8, “Rules and tuning for the UEBA app,”](#) on page 83.

About this task

Restriction: Do not customize your rules to use the UEBA and Machine Learning reference sets. Attempting to use the reference sets in custom rules can lead to failures within the UEBA app.

If the rule works on flow data, you must enable the **Search assets for username, when username is not available for event or flow data** option so that events with no usernames can attempt a lookup for user mapping.

The risk score maximum limit is configured in the Application Settings section on the UEBA Settings page. For more information, [“Configuring application settings” on page 32.](#)

- [“Integrating content without QRadar Use Case Manager \(or QRadar Use Case Manager 3.1.0 or earlier\)” on page 63](#)
- [“Integrating content with Use Case Manager 3.2.0 or later” on page 63](#)

Integrating content without QRadar Use Case Manager (or QRadar Use Case Manager 3.1.0 or earlier)

About this task

Complete the procedure if any one of the scenarios applies:

- You are not using any version of QRadar Use Case Manager.
- You are using an older version of QRadar Use Case Manager (3.1.0 or earlier).
- You are on an unsupported version of UEBA (more than two versions back from the current released version).

Procedure

1. Create a copy of the existing rule. Making a copy of an existing rule prevents updates to the base rule from affecting the edits that are made to the new rule.
2. Open the rule in the **Rule Wizard** and then go to the Rule Response section.
3. Enable or edit the **Dispatch New Event** option by making sure that the **Event Description** text is formatted in the following way: `senseValue=#`
4. Click **Finish** to save the changes.

Integrating content with Use Case Manager 3.2.0 or later

About this task

Complete the procedure if both of the following conditions apply:

1. You are using [QRadar Use Case Manager 3.2.0 or later](#).
2. You are using a supported version of UEBA.



Attention: When you upgrade to UEBA 4.1.0 or later and [QRadar Use Case Manager 3.2.0 or later](#), you manage rules in [QRadar Use Case Manager](#), and no longer manage rules in the UEBA **Rules and Tuning** page. For more information, see [QRadar Use Case Manager](#).

Procedure

1. Create a duplicate of the existing rule. Making a duplicate of an existing rule prevents updates to the base rule from affecting the edits that are made to the new rule.
2. Select the rule to open the details page and then select **User Behavior Analytics risk score**.
3. Enter the score and wait for it to save.

Tuning entity assets

Entity refers to devices, asset IP address, hostname, and MAC address in your environment.

About this task

The Asset Model component in QRadar is used to track the devices and assets available in QRadar. Ensure that your asset model is updated to reflect the correct assets.

Procedure

1. Manage Asset Auto discovery by using exclusions. See [QRadar: How to effectively manage Asset Autodiscovery using exclusions](#).
2. Maintain a proper blacklist and allowlist. See [Asset blacklists and allowlists](#).
3. Use Integrate Virtual Appliance scanner for better visibility of vulnerability information on UEBA.
4. Select **Advanced** in **Asset Profiler Retention Period**, and set the same days (7 to 15 days) for all criteria.

UEBA common challenges

This topic describes the common challenges UEBA users face and the best practices to address these challenges.

- [“User Coalescing – Multiple LDAP fields are used for aliases” on page 64](#)
- [“Display Fields – Multiple fields are configured for Display name and Full name” on page 65](#)
- [“User Discovery – users discovered from events vs users imported from active directory” on page 66](#)
- [“LDAP Filters – Setting a wrong filter or no filter could lead to a large amount of identities getting imported to UEBA” on page 67](#)
- [“Enabling Index – Having this disabled could lead to search performance issues and overall app slowness” on page 68](#)

User Coalescing – Multiple LDAP fields are used for aliases

Complete the procedure to address this challenge:

1. Identify one or two aliases/attributes for users that are unique across all ADs.
2. Start small and then add more attributes if needed.
3. Recommended attributes:
 - sAMAccountName
 - uid
 - userPrincipalName
 - cn
 - mail

Note: The procedure can also improve UEBA performance due to less user records.

User coalescing

Select the attributes from the current imports, which UBA can use to identify and combine activity from different department or country, causes UBA to combine all users with the same department or country value.

Aliases

samaccountname uid userprincipalname cn mail distinguishedname objectsid [Edit](#)

Display Fields – Multiple fields are configured for Display name and Full name

The inconsistent use of **Display name** and **Full name** can cause confusions. Complete the procedure to address this challenge:

1. Identify the correct attribute against each field which should display in the user profile.
2. If *distinguishedname* and *displayname* attribute are used for **Display name** then the **Display name** will use *distinguishedname* attribute if available.
3. Display name uses first available attribute in order.

Display fields

Select the attributes from the current imports to be displayed on the user profile page. You can select all, some, or none of the display attributes depending on the display attributes. "Display Name" is the main username displayed on the UBA dashboard for each user. "Custom Group" can be used to specify another selection from your imports when you configure the Defined Peer Group analytic in the Machine Learning app.

Display name	displayname distinguishedname cn samaccountname mailnickname userprincipalname name givenname Edit
Full name	cn samaccountname mailnickname userprincipalname distinguishedname displayname name givenname Edit
Email	mail Edit
Job title	title description Edit
Manager	manager managedby Edit
Department	department ou Edit
Group membership	memberof Edit
City	l Edit
State	st Edit

CN=dkelly, OU=sales-market10

Full name: group_C-25_ariel_C_log_C
Email: group_C-25_ariel_C_log_C@example.ibm.com
Job title: Sales Manager (67 peers)
Department: Marketing (79 peers)
Location: Yokohama, Kanagawa, Japan (7 peers)

Active
group_C-25_ariel_C_log_C

Never used
group_C-25_ariel_C_log_C@example.ibm.com

Overview / User details

Debra Kelly

Full name: [group_C-25_ariel_C_log_C](#)
Email: group_C-25_ariel_C_log_C@example.ibm.com
Job title: [Sales Manager \(67 peers\)](#)
Department: [Marketing \(79 peers\)](#)
Location: [Yokohama, Kanagawa, Japan \(7 peers\)](#)

Active
[group_C-25_ariel_C_log_C](#)

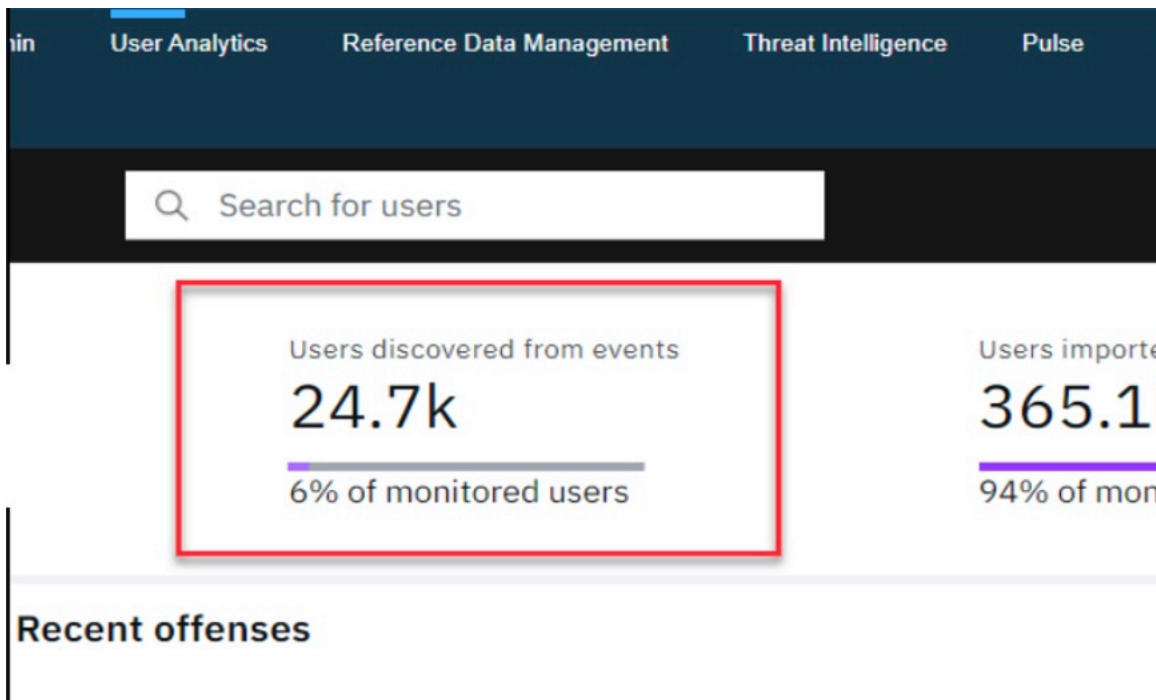
Never used
group_C-25_ariel_C_log_C@example.ibm.com

User Discovery – users discovered from events vs users imported from active directory

Complete the procedure to address this challenge:

- Enable the **Monitor imported user only** setting in **QRadar Settings**, if your use case requires you to monitor AD imported users.

Note: The procedure is also useful when you only recently started using UEBA. Once you have all the needed users imported from AD, you may then want to discover users from events and monitor risks.



The screenshot shows the 'UBA Settings' interface. It is divided into three main sections: 'QRadar Settings', 'Content Package Settings', and 'Application Settings'. The 'Application Settings' section is highlighted with a red border. In this section, the 'Monitor imported users only' toggle is turned off. Below it, the 'Risk threshold' is set to 'Dynamic' with a current value of 70. A text input field for the 'Dynamic threshold' contains the number '4'. The 'Generate an offense for high risk users' toggle is also turned off. A 'Save Configuration' button is located at the bottom right of the settings area.

LDAP Filters – Setting a wrong filter or no filter could lead to a large amount of identities getting imported to UEBA

Complete the procedure to address this challenge:

1. Set LDAP filters in **LDAP server configuration**. For example:
 - (objectClass=person) : All users and service accounts will be coalesced.
 - (objectClass=user) : Only user accounts will be coalesced.
2. For more information about constructing LDAP filters, see <https://ldap.com/ldap-filters/>.

Note:

- Default Retrieval Limit: UBA retrieves users in chunks and default settings is 500,000.
- Slow LDAP connection can cause timeouts.
- Set the chunk size to around 100,000 to retain system stability.

User Import > Add

1 LDAP server configuration

2 Other import settings

3 Summary

LDAP server configuration

Enter the LDAP server information to retrieve user data. Before going to the next step, click Test connection.

Protocol: ldap://

LDAP server host *: example.ldap.com

Port *: 389

Enter a valid IP address or hostname.

Username (Bind DN):

Password:

Advanced settings

Base DN: dc=example,dc=ldap,dc=com

Filter: (objectClass=person)

Certificate: Click to upload the certificate file for the root certificate authority. File size is limited to 10 KB.

Paged results

Test connection

Synchronize reference table

Enable to update reference table with user imported data.

Polling interval *

Enter 0 for manual poll or set the polling interval with value between 8 and 8640. 24 Hours

Retrieval limit *

Enter an integer value between 1 and 500000. 500,000 Users

Enabling Index – Having this disabled could lead to search performance issues and overall app slowness

Complete the procedure to address this challenge:

- Enable **Index** in QRadar to optimize system performance.

Enable Index Disable Index High Level Category

Display: Last 24 Hours View: All Database: All Show: All

Index management allows you to control database indexing, which can optimize search performance for frequently used criteria. The system supports multiple indexed properties. Properties that can be indexed in the system are listed below.

WARNING: Enabling indexing on too many properties, can have a negative impact on system performance. It is important that you return to this page after adjusting indexing to monitor the health of the indexes.

Indexed	Property	% of Searches Using Property	% of Searches Hitting Index	% of Searches Missing Index	Data Written	Database
<input checked="" type="checkbox"/>	High Level Category	63.13%	82.8%	17.2%	17MB	events

Reference sets

The User Entity Behavior Analytics (UEBA) app and the Machine Learning app use reference sets for storing user information. Some reference sets are reserved for app use only and you should not modify them or use them in creating custom rules.

Reference sets you can customize

Reference set	Description
UBA : High Risk Users	The <i>UBA : High Risk Users</i> reference set is built from the Risk threshold to trigger offenses value on the UBA Settings page. The maximum number of users is 10,000 and the reference set is rebuilt every 5 minutes
UBA : Trusted Usernames	You can add user names to the <i>UBA : Trusted Usernames</i> reference set but do not use for rules or reports. No offenses are generated for the users in the <i>UBA : Trusted Usernames</i> reference set.
UBA : Users Not Tracked	<p>The purpose of the <i>UBA : Users Not Tracked</i> reference set is to store the list of user's aliases that no longer require tracking because of General Data Protection Regulation (GDPR) regulations. When you choose to stop tracking users and click Delete and Stop Tracking User on the user details page, the user name or alias is added to this reference set.</p> <p>Important: Do not manually add users to or modify the <i>UBA : Users Not Tracked</i> reference set.</p> <p>Note: If you need to start tracking a user after the name has been added to the reference set, you can delete the user's aliases from the reference set.</p> <p>Use the Reference Set Management page to delete users. For more information, see Deleting elements from a reference set.</p>
UBA : ML Always Tracked Watchlist	The <i>UBA : ML Always Tracked Watchlist</i> reference set is built from the users you select to Track with Machine Learning in the Advanced Settings section on the User Details page. You can add user names to the <i>UBA : ML Always Tracked Watchlist</i> reference set but do not use for rules or reports.
UEBA: Entities Not Tracked	<p>The purpose of the <i>UEBA: Entities Not Tracked</i> reference set is to store the list of asset IDs that no longer require tracking because of GDPR regulations. When you choose to stop tracking users and click Delete and Stop Tracking User on the user details page, the user name or alias is added to this reference set.</p> <p>Important: Do not manually add asset IDs to or modify the <i>UEBA: Entities Not Tracked</i> reference set.</p> <p>Note: If you need to start tracking an entity after the name is added to the reference set, you can delete the asset ID of the entity from the reference set.</p> <p>To get asset ID of an entity, you can search asset IP or assets MAC address or hostname in Assets module of QRadar. Use the Reference Set Management page to delete entities. For more information, see Deleting elements from a reference set</p>

Reference sets you cannot customize

Restriction: Do not modify or use the following reference sets for custom rule creation.

- UBA - Current ML Tracked Users
- UBA - Previous ML Tracked Users

- UBA - Current Abridged ML Tracked Users
- UBA - Previous Abridged ML Tracked Users
- UBA - Current Peer Group ML Tracked Users
- UBA - Previous Peer Group ML Tracked Users

Chapter 7. Multitenancy in UEBA

The User Entity Behavior Analytics (UEBA) app supports multitenant environments in QRadar. You can create multiple tenants from a single deployment instead of managing multiple deployments.

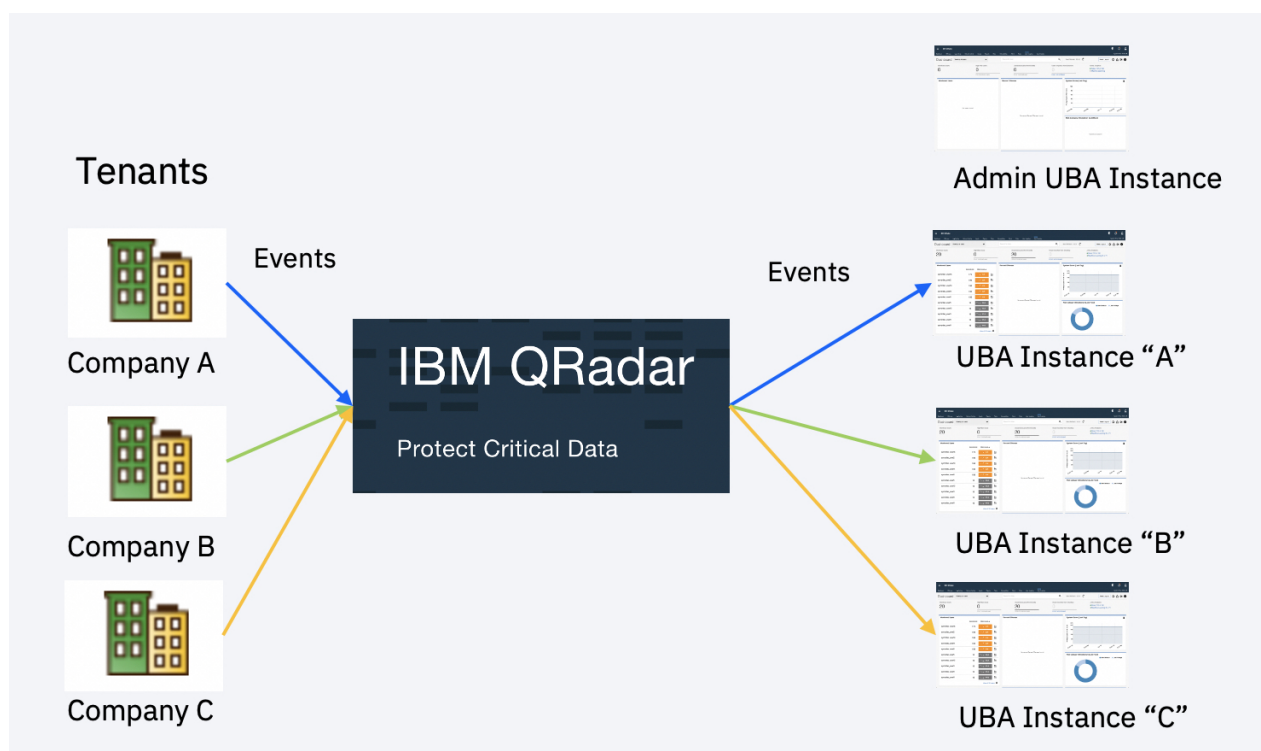
Multitenant environments allow Managed Security Service Providers (MSSPs) and multi-divisional organizations to provide security services to multiple client organizations from a single, shared IBM QRadar deployment. You don't have to deploy a unique QRadar instance for each customer.

You can create multiple tenants from a single deployment instead of managing multiple deployments. For example, as an MSSP partner, you might host 20 clients on a single instance of QRadar with each client managing approximately 1000 employees.

Important: When you are logged in to QRadar as an MT site admin, by default you see two tenants, one of which is the Admin tenant. Use the IBM QRadar Hub app to modify which other tenant you see by default.

Overview

Multitenancy in UEBA requires the QRadar Administrator or an MSSP Administrator (QRadar Admin) to complete several setup procedures that include specific configuration tasks in supported versions of QRadar. The QRadar Admin must use the IBM QRadar Hub app 3.0 or later to install and configure the first or "admin" UEBA instance and the additional non-admin or tenant instances. After the non-admin instances are established, the QRadar Admin must also assign user roles and specific permissions. The user roles for the non-admin instances include "UEBA tenant admin" and "UEBA tenant" users.



Deployment guidance

The number of UEBA instances that are supported is directly related to the QRadar environment. In general, tenants should be added one at a time and after each addition, you should verify that QRadar is healthy and the remaining apps are also performing as expected.

QRadar system performance was confirmed on three different environments that differed in the number of users and Events Per Second (EPS). Each environment contained a QRadar Console with 128 GB RAM

and 56 Cores, Event Processor with 128 GB RAM and 56 Cores, and an App Host with 372 GB RAM and 72 Cores.

- The first system successfully ran 30 instances of UEBA with 5000 users on each instance with an EPS of 800.
- The second system successfully ran 8 instances of UEBA with 40000 users on each instance with an EPS of 1500.
- The third system successfully ran 6 instances of UEBA with 100000 users on each instance with an EPS of 2500.

These guidelines ensure the proper functioning of your QRadar system and UEBA. If errors are encountered within your QRadar environment, consider increasing RAM or adding an Event Processor.

QRadar Admin or MSSP Admin role

Important: The QRadar Admin must set up the first or "admin" instance of UEBA. After the admin instance of UEBA is established with an admin token, more UEBA instances can then be created. When running multiple instances of UEBA, the admin instance is used solely to upgrade Machine Learning (ML app) and install content but it does not process data or perform any other functions. Do not remove the admin instance.

Security profiles

UEBA does not support multiple domains under one security profile. A security profile can only have one domain assigned to it for UEBA to work as expected.

Dashboard

On the Dashboard, only the QRadar Admin can see the rules installation status for the UEBA tenant admin user and the UEBA tenant user. The UEBA tenant admin user and the UEBA tenant user always see a green status of rules on the dashboard.

If you have Machine Learning (ML app) installed, the status for Machine Learning on the Dashboard is always shown as green. If you do not have the ML app installed, the status that is shown is always gray.

Integration with QRadar Advisor with Watson

If you want to integrate QRadar Advisor with Watson in a UEBA multitenant environment, you should install QRadar Advisor with Watson version 2.5.2 or later.

Reference Data Import - LDAP app

You should not use the LDAP app in a multitenant environment because the LDAP app is not multi-domain or multitenant aware so any user will see any import.

Moving from a single instance of UEBA to multiple instances

For the best experience with multitenancy, it is recommended to start with a fresh installation of UEBA.

If you are moving from a single instance of UEBA to a multitenant setup, you will not be able to keep using the existing UEBA instance and also run multitenancy. As soon as a second instance of UEBA is seen in QRadar, the upgraded UEBA instance will change into a limited-functionality instance. Note that the data is not removed but it no longer gets updated. You also must uninstall the ML app before installing any additional instances.

Important: Do not uninstall the Admin or shared instance.

Upgrading

To upgrade UEBA with a multitenant setup, you should apply the upgrade to the Admin instance. All of the tenant instances will be upgraded along with it.

Warnings

You must set up your multitenant environment as specified or you could experience problems with UEBA and Machine Learning. Consider the following warnings:

- Do not uninstall the Admin or shared instance.
- Ensure any edits to reference sets in QRadar are domain specific, otherwise users might show up in unintended tenant instances.
- Do not install Machine Learning (ML app) on the admin instance of UEBA.
- The admin instance of UEBA is only responsible for updating rules and informing other (non-admin) instances about Machine Learning updates.
- The admin instance of UEBA will not ingest user data.
- Each instance can only have a single tenant and each tenant can only have a single domain.
- Tenants cannot be provided an admin authorized service token.
- The QRadar Admin should not add users to the trusted users list or remove users because it will also add trusted users and remove users for all tenant instances.

QRadar configurations for setting up multitenancy in UEBA

You must configure your QRadar system to support UEBA 3.6.0 and later in a multitenant environment.

You must have QRadar administrator privileges to set up your multitenant environment. For more information, see [QRadar administration](#).

For more information about multitenancy in QRadar, see [Multitenant management](#).

Table 4. QRadar configurations to support UEBA multitenancy. The following table outlines the steps that must be completed before you begin to configure your UEBA instances. The steps outlined in the table are executed from the QRadar Admin settings.

Step		More information
1	Define IBM Sense log source for each domain. (System Configuration > Data Sources > Log sources)	Each domain requires its own IBM Sense log source for each UEBA instance to function properly. Important: When the log source is defined, take note of each unique IBM identifier for use when configuring the tenant UEBA instance. The identifier that is used in creating the IBM Sense log source for each instance is also added to the settings for each instance. This identifier tells the UEBA instance which log source will be used in processing its sense events. Note: Only the first or "admin" instance of UEBA will have an IBM Sense log source created by default. You must create an IBM Sense log source for additional UEBA tenants. Domains and log sources in multitenant environments
2	Optional: Determine data provisioning. (System Configuration > Data Sources > Log Source Groups)	You can assign specific log sources, log source groups, or event collectors to provide data for each domain. You can create the log source groups. Assign the IBM Sense from step one to the specific group if one is created.

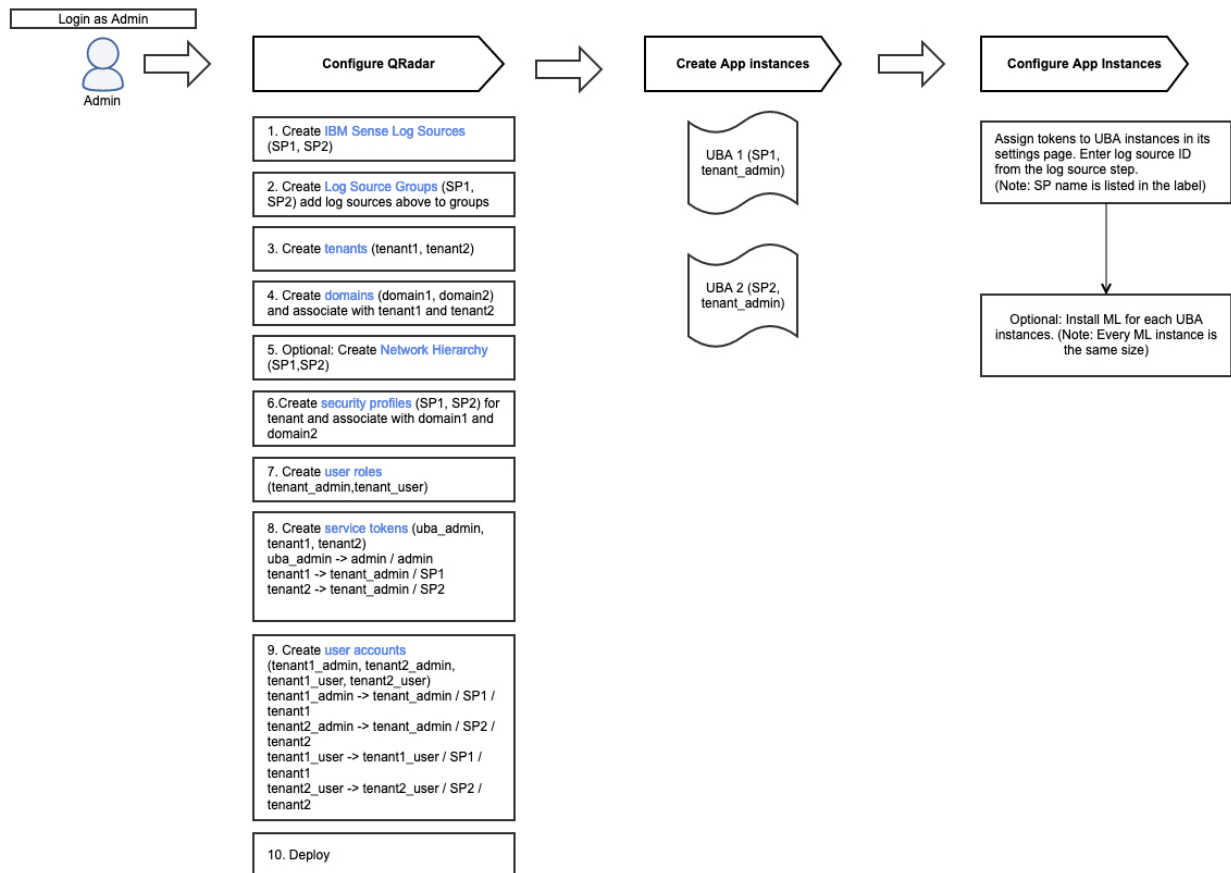
Table 4. QRadar configurations to support UEBA multitenancy. The following table outlines the steps that must be completed before you begin to configure your UEBA instances. The steps outlined in the table are executed from the QRadar Admin settings. (continued)

Step		More information
3	Define a set of tenants in Tenant Management (System Configuration > User Management > Tenant Management)	Provisioning a new tenant
4	Define a set of domains in Domain Management (System Configuration > Domain Management)	Associate the IBM Sense log source from step 1 (if log source groups are not used), and log source groups, logs sources, or event collectors from step 2. Add a tenant from step 3. Each domain must have a unique tenant and log source or log source group. Creating domains
5	Optional: Define networks in Network Hierarchy (System Configuration > Network Hierarchy)	Note: This is only necessary if you want each tenant to have specific network hierarchy Network hierarchy updates in a multitenant deployment
6	Create a profile for each domain in Security Profiles (System Configuration > User Management > Security Profiles)	Associate the previously defined domain, log source, or log source group, and network. Note: Permission precedence must be set to No restrictions. Security profiles
7	Create roles in User Roles and then deploy changes. (System Configuration > User Management > User Roles)	QRadar admin/MSSP admin: Install and configure each UEBA and Machine Learning instance. See “QRadar admin/MSSP admin” on page 78 for details. Tenant admin: UEBA Admin role for administering a UEBA and Machine Learning instance. See “UEBA tenant admin” on page 78 for details. Tenant user: UEBA Analyst role for reviewing data in UEBA. See “UEBA tenant user” on page 79 for details. Note: User Entity Analytics, Machine Learning, and QRadar Advisor with Watson might not be available at this point. On the Admin tab, click Deploy changes . User roles
8	Create service tokens in Authorized Services (System Configuration > User Management > Authorized Services)	Associate to profile from step 6 and role from step 7. Each tenant admin requires an authorization service token. “Configuring the authorization token in QRadar settings” on page 31
9	Create users in Users (System Configuration > User Management > Users)	Create tenant admin and tenant users. Associate each to the specific role, profile, and tenant. Creating a user account

Table 4. QRadar configurations to support UEBA multitenancy. The following table outlines the steps that must be completed before you begin to configure your UEBA instances. The steps outlined in the table are executed from the QRadar Admin settings. (continued)

Step		More information
10	Deploy changes	On the Admin tab, click Deploy changes .

The following diagram illustrates the configuration steps:



Related concepts

[UEBA user roles for multitenancy](#)

The User Entity Behavior Analytics (UEBA) app 3.6.0 and later supports multitenant environments in QRadar 7.4.3 Fix Pack 6 and later.

[Rules and tuning for multitenancy in UEBA](#)

The rules are enabled or disabled by default for every UEBA instance to support multitenancy in User Entity Behavior Analytics (UEBA) app 3.6.0 and later. If you require changes to rules for a subsets of instances, you need to manually change the rule behavior.

Related tasks

[Installing and configuring UEBA instances to support multitenancy](#)

You can set up UEBA to work in a multitenant environment in QRadar 7.4.3 Fix Pack 6 or later.

[Installing and configuring Machine Learning in Multitenancy](#)

With 3.6.0 and later, you can install and configure Machine Learning to work in a multitenant environment in QRadar 7.4.3 Fix Pack 6 and later.

Installing and configuring UEBA instances to support multitenancy

You can set up UEBA to work in a multitenant environment in QRadar 7.4.3 Fix Pack 6 or later.

Before you begin

You must complete the steps that are outlined in the table on the [“QRadar configurations for setting up multitenancy in UEBA”](#) on page 73 page on a system with QRadar 7.4.3 Fix Pack 6 or later.

Before you attempt to configure any UEBA instance, make sure you have an Admin instance of UEBA installed by completing the following steps [“Installing the User Entity Behavior Analytics app”](#) on page 25.



Attention:

- Installing instances requires IBM QRadar Hub app 3.0.0 or later. For more information, see [IBM QRadar Hub](#).
- Do not uninstall the Admin or shared instance.

About this task

The following procedure must be completed by the QRadar Admin or the MSSP admin.

Procedure

1. Find the User Entity Behavior Analytics extension in the IBM QRadar Hub app.

Installed Extensions



ID	Name	Status	Version	Number of Instances	Total Memory	Installed By	Install Date	Options
801	User Behavior Analytics	Running	3.6.3757	1	3000 MB	admin	Apr 08, 2020	...
Instance Name	Status	Security Profile	Memory	Created By	Creation Date	Options		
User Behavior Analytics-shared	Running	shared	3000 MB	uba_admin	Apr 02, 2020	...		

2. Select **Options** > **Create new instance**.
3. Choose the security profile for the instance and click **Next**.

Note: If there are no instances created, create an Admin instance first. If there is an Admin or Shared instance, create the first tenant instance. If the tenant security profile is not listed, ensure that you have created a security profile and deployed changes.
4. Associate the app to any other roles that are listed and click **Next**.
5. Review the summary and click **Confirm and Create**.
6. After the instance is created, select the instance and then click **Options** > **Configure Instance** > **UBA Settings**.
7. On the **UBA Settings** page, add the service token for the tenant admin that is responsible for the instance of UEBA. Note: Make sure to choose the correct token.
8. Enter the identifier set for the IBM Sense log source for this instance's domain. For more information, see step 1 of [QRadar configurations for setting up multitenancy in UBA](#).
9. Save the configuration.
10. Optional: If this instance of UEBA will also host Machine Learning, see the following topic [“Installing and configuring Machine Learning in Multitenancy”](#) on page 77.

What to do next

Repeat these steps for all instances of UEBA that you want.

Related concepts

[QRadar configurations for setting up multitenancy in UEBA](#)

You must configure your QRadar system to support UEBA 3.6.0 and later in a multitenant environment.

[UEBA user roles for multitenancy](#)

The User Entity Behavior Analytics (UEBA) app 3.6.0 and later supports multitenant environments in QRadar 7.4.3 Fix Pack 6 and later.

[Rules and tuning for multitenancy in UEBA](#)

The rules are enabled or disabled by default for every UEBA instance to support multitenancy in User Entity Behavior Analytics (UEBA) app 3.6.0 and later. If you require changes to rules for a subsets of instances, you need to manually change the rule behavior.

Related tasks

[Installing and configuring Machine Learning in Multitenancy](#)

With 3.6.0 and later, you can install and configure Machine Learning to work in a multitenant environment in QRadar 7.4.3 Fix Pack 6 and later.

Installing and configuring Machine Learning in Multitenancy

With 3.6.0 and later, you can install and configure Machine Learning to work in a multitenant environment in QRadar 7.4.3 Fix Pack 6 and later.

Before you begin

You must complete the steps outlined in the table on the [“QRadar configurations for setting up multitenancy in UEBA”](#) on page 73 page on a system with QRadar 7.4.3 Fix Pack 6 and later.

Before attempting to install and configure any Machine Learning instance be sure you have an Admin instance of UEBA installed by completing the following steps [“Installing the User Entity Behavior Analytics app”](#) on page 25.



Attention: Do not install Machine Learning (ML app) on the Admin or shared instance.

About this task

The following procedure must be completed by the QRadar Admin or the MSSP admin.

Important: For QRadar version 7.4.3, the container size and the amount of memory you select for the first Machine Learning instance that you configure will apply to all tenant instances. To change the container size, you would need to remove all running Machine Learning instances and install again to be able to configure a different container size. For QRadar 7.5.0, the first Machine Learning instance created will become the lowest available container size allowed for additional tenants. Additional tenants will be allowed to specify a container size greater than the first Machine Learning instance.

Procedure

1. Find the User Entity Behavior Analytics extension in the IBM QRadar Hub app.
2. Select the UEBA instance that you want to install Machine Learning on.
3. Select **Option > Configure Instance > Machine Learning Settings**.
4. Configure the appropriate size for the Machine Learning instance.

Important:

- QRadar 7.4.3: The size of the Machine Learning instance must be the same for every instance when using QRadar 7.4.3. For example, if instance A uses a 5 GB Machine Learning instance, instances B and C must either use no Machine Learning or 5 GB.
- QRadar 7.5.0: For QRadar 7.5.0 each tenant is allowed to be equal or greater than the size of the initial Machine Learning instance. For example, if instance A uses 5 GB, then instance B and C may install 5 GB or larger, but are not permitted to install at 2 GB size.

5. Select **Install ML App**.

The instance is now ready for the tenant admin and tenant users to access.

What to do next

Repeat these steps for instances of UEBA that you want to install Machine Learning on.

Related concepts

[QRadar configurations for setting up multitenancy in UEBA](#)

You must configure your QRadar system to support UEBA 3.6.0 and later in a multitenant environment.

[UEBA user roles for multitenancy](#)

The User Entity Behavior Analytics (UEBA) app 3.6.0 and later supports multitenant environments in QRadar 7.4.3 Fix Pack 6 and later.

[Rules and tuning for multitenancy in UEBA](#)

The rules are enabled or disabled by default for every UEBA instance to support multitenancy in User Entity Behavior Analytics (UEBA) app 3.6.0 and later. If you require changes to rules for a subsets of instances, you need to manually change the rule behavior.

Related tasks

[Installing and configuring UEBA instances to support multitenancy](#)

You can set up UEBA to work in a multitenant environment in QRadar 7.4.3 Fix Pack 6 or later.

UEBA user roles for multitenancy

The User Entity Behavior Analytics (UEBA) app 3.6.0 and later supports multitenant environments in QRadar 7.4.3 Fix Pack 6 and later.

In a multitenant deployment, you ensure that customers see only their data by creating domains that are based on their QRadar input sources. By creating security profiles and user roles, you can manage privileges for large groups of users within the domain. User roles ensure that users have access to only the information that they are authorized to see.

Note: UEBA 3.6.0 (and later) does not support multiple domains under one security profile. A security profile can only have one domain assigned to it in order for UEBA to work as expected.

For UEBA to work with QRadar, the QRadar Admin can create user roles that designate a "UEBA tenant admin" and any non-admin users or "UEBA tenant". Each role has distinct responsibilities and associated activities.

QRadar admin/MSSP admin

The QRadar Admin/MSSP admin owns and manages the first or "admin" instance of UEBA. The QRadar admin is responsible for completing the following tasks:

- Setting up the first "admin" instance and the other non-admin UEBA instances.
- Configuring non-admin instances with the appropriate tenant_admin token and instance identifiers
- Determining the size and installing Machine Learning for any instance that requires it. Note: The size of the Machine Learning instance must be the same for every instance. For example: If instance A uses a 5 GB Machine Learning instance, instances B and C must either use no Machine Learning or also 5 GB.
- Upgrading all apps or systems.
- Managing all system settings and rule configurations. Note: Rules are shared for every instance.

UEBA tenant admin

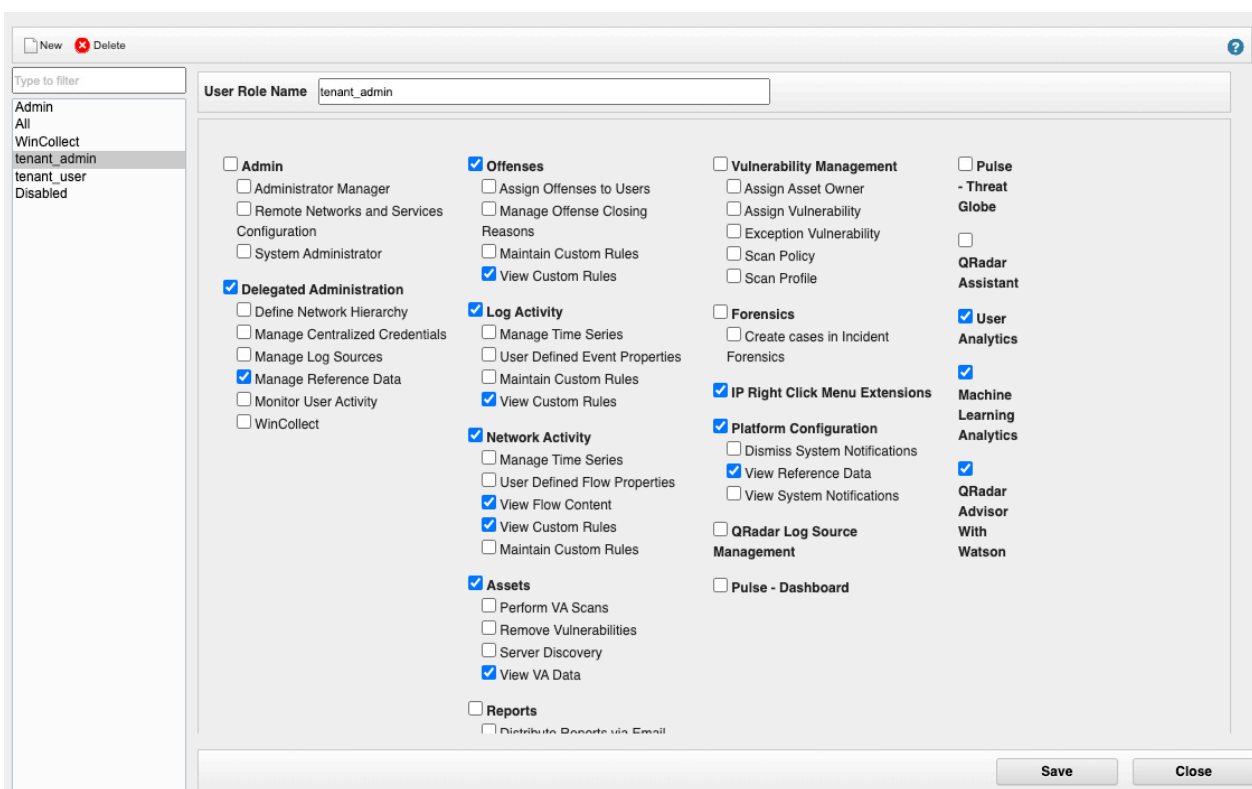
The UEBA tenant admin is responsible for the following tasks:

- Configuring UEBA Settings (specifically Application Settings)
- Configuring Machine Learning settings.

- Adding users to the trusted user list and deleting users.
- Setting the Machine Learning priority.
- Investigating users with QRadar Advisor with Watson.
- Configuring user imports.
- Creating domain filters.
- Creating and enabling custom machine learning models.
- Creating GDPR reports.

Complete the following procedure to create a role for the tenant admin user.

1. On the navigation menu (☰), click **Admin**.
2. In the System Configuration section, click **User Management**, and then click the **User Roles** icon.
3. Create a new role for the tenant admin user. For example, tenant_admin.
4. Select the checkboxes as indicated in the following screen shot to add the permissions to the role.
5. Click **Save**.



UEBA tenant user

The UEBA tenant user has limited ability to manage the UEBA instance but can do the following:

- View and analyze user data in UEBA.
- Internally investigate users.

Complete the following procedure to create a role for the UEBA tenant user.

1. On the navigation menu (☰), click **Admin**.
2. In the System Configuration section, click **User Management**, and then click the **User Roles** icon.
3. Create a new role for a tenant user. For example, tenant_user.
4. Select the checkboxes as indicated in the following screen shot to add the permissions to the role.

5. Click **Save**.

The screenshot shows the QRadar configuration interface for a user role named "tenant_user". The interface is divided into a left sidebar with a role list and a main configuration area. The role list includes "Admin", "All", "WinCollect", "tenantAdmin", "tenant_user" (selected), and "Disabled". The main configuration area is titled "User Role Name" and contains a grid of checkboxes for various configuration options. The checked options are: Offenses (Assign Offenses to Users, View Custom Rules), Log Activity (View Custom Rules), Network Activity (View Custom Rules), Assets (View VA Data), and Machine Learning Analytics. The unchecked options include: Admin (Administrator Manager, Manage Local Only, Authentication Setting, Remote Networks and Services Configuration, System Administrator), Delegated Administration (Define Network Hierarchy, Manage Centralized Credentials, Manage Log Sources, Manage Reference Data, Monitor User Activity, WinCollect), Risk Manager, Vulnerability Management (Assign Asset Owner, Assign Vulnerability, Exception Vulnerability), Read-only Configuration (View Log Sources, View Offenses, View User Roles, View Users), Pulse - Dashboard, QRadar Assistant, User Analytics, Machine Learning Analytics, Forensics (Create cases in Incident Forensics), IP Right Click Menu Extensions, Platform Configuration (Dismiss System Notifications, View Reference Data, View System Notifications), Reports (Distribute Reports via Email, Maintain Templates), and Perform VA Scans, Remove Vulnerabilities, Server Discovery.

Related concepts

[QRadar configurations for setting up multitenancy in UEBA](#)

You must configure your QRadar system to support UEBA 3.6.0 and later in a multitenant environment.

[Rules and tuning for multitenancy in UEBA](#)

The rules are enabled or disabled by default for every UEBA instance to support multitenancy in User Entity Behavior Analytics (UEBA) app 3.6.0 and later. If you require changes to rules for a subsets of instances, you need to manually change the rule behavior.

Related tasks

[Installing and configuring UEBA instances to support multitenancy](#)

You can set up UEBA to work in a multitenant environment in QRadar 7.4.3 Fix Pack 6 or later.

[Installing and configuring Machine Learning in Multitenancy](#)

With 3.6.0 and later, you can install and configure Machine Learning to work in a multitenant environment in QRadar 7.4.3 Fix Pack 6 and later.

Rules and tuning for multitenancy in UEBA

The rules are enabled or disabled by default for every UEBA instance to support multitenancy in User Entity Behavior Analytics (UEBA) app 3.6.0 and later. If you require changes to rules for a subsets of instances, you need to manually change the rule behavior.

The following procedure must be completed by the QRadar Admin or the MSSP admin.

By default, all rules are either enabled or disabled for every instance of UEBA. If you have a need to make any rule function for a subset of the instances, you will need to edit the rule as follows:

1. Make a copy of the rule and rename the rule and event to fit the situation. For example, if Domain1 wants the rule "UBA : Terminated User Activity" enabled while the others do not, copy the rule and rename it "UBA : Terminated User Activity Domain1". Rename the event the same.
2. In the new rule, add the test "when the domain is one of the following" and select the domains it should apply to. Move the test to the top of the list.

3. If the rule is one that writes out to some reference data, change the setting from Shared Data to Domain Specific.
4. Make sure the new rule is enabled.
5. Save the rule.
6. Make sure the original rule is disabled. Note: You should exclude the intended domain from the original rule if the rule is still needed after the copy is created.

Known issue

In QRadar 7.4.0 Fix Pack 1, there is no way to make the rule limiter domain aware. Each rule that applies to more than a single domain will be limited across domains. For example, if Domain1 and Domain2 both have a "John Doe" that triggers the same rule within the limitation time frame, only one of the users will be flagged by the rule.

Related concepts

[QRadar configurations for setting up multitenancy in UEBA](#)

You must configure your QRadar system to support UEBA 3.6.0 and later in a multitenant environment.

[UEBA user roles for multitenancy](#)

The User Entity Behavior Analytics (UEBA) app 3.6.0 and later supports multitenant environments in QRadar 7.4.3 Fix Pack 6 and later.

Related tasks

[Installing and configuring UEBA instances to support multitenancy](#)

You can set up UEBA to work in a multitenant environment in QRadar 7.4.3 Fix Pack 6 or later.

[Installing and configuring Machine Learning in Multitenancy](#)

With 3.6.0 and later, you can install and configure Machine Learning to work in a multitenant environment in QRadar 7.4.3 Fix Pack 6 and later.

Chapter 8. Rules and tuning for the UEBA app

The IBM QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

The User Entity Behavior Analytics (UEBA) app includes use cases that are based on custom rules. These rules are used to generate data for the UEBA app dashboard. You can view, filter, and tune rules within the IBM QRadar Use Case Manager app. For information about integrating QRadar content, see [“Integrating new or existing QRadar content with the UEBA app”](#) on page 62.

Restriction: Do not customize your rules to use the UEBA and Machine Learning reference sets. Attempting to use the reference sets in custom rules can lead to failures within the UEBA app. For more information, see [“Reference sets”](#) on page 69.

For more information about working with rules in QRadar Use Case Manager, see [QRadar Use Case Manager app](#).

For more information about working with rules in QRadar, see [Rules](#).

For more information about enabling Machine Learning user models, see [Chapter 10, “Machine Learning user models,”](#) on page 247.

UEBA content pack summary

When you install the UEBA app, content packages that contain UEBA-specific rules are also installed. The content packages and the count details are listed.

UEBA-specific content packages, which contain rules for sending sense events, are installed as separate extensions. Content packages are installed by default. If you choose to create your own custom rules that send sense events to UEBA, you can change the **Install and upgrade content packages** setting when you configure UEBA Settings.

Note: Not all content in each package is unique. The counts for custom rules will not match the number of rules seen on the **Rules and Tuning** page. These counts include building blocks and other helper rules.

Table 5. Content packages and counts

Content Pack	Custom Rules	Reference Data	Custom Properties	Property Expressions	QID Records
Access and Authentication	37 42 (UEBA 4.1.0)	15	4	9	22 25 (UBA 4.1.0)
Accounts and Privileges	32	5	2	9	12
Browsing Behavior	20	0	2	14	19
Cloud	16	2	5	6	12
DNS Analyzer	5	0	0	0	4
Domain Controller	15	5	13	26	11

Table 5. Content packages and counts (continued)

Content Pack	Custom Rules	Reference Data	Custom Properties	Property Expressions	QID Records
Endpoint	24 (UEBA 3.7.0) 22 (UEBA 3.8.0)	7 (UEBA 3.7.0) 6 (UEBA 3.8.0)	10	17 (UEBA 3.7.0) 38 (UEBA 3.8.0)	13 (UBA 3.7.0) 12 (UBA 3.8.0)
Exfiltration	24 27 (UEBA 4.1.0)	1	3	17	11 12 (UBA 4.1.0)
Geography	12	4	0	0	7
MaaS360	10	0	0	0	10
Network Traffic	3 (UEBA 3.7.0) 4 (UEBA 3.8.0)	2	1 (UEBA 3.7.0) 2 (UEBA 3.8.0)	3 (UEBA 3.7.0) 8 (UEBA 3.8.0)	3 (UBA 3.7.0) 4 (UBA 3.8.0)
Threat Intelligence	19	6	7	17	14

UEBA 5.x rules

The following rules are modified for UEBA 5.x.

1. [“UEBA : Dormant Account Used” on page 118](#)
2. [“UEBA : Large number of denied access events towards external domain” on page 91](#)
3. [“UEBA : Remote access hole in corporate firewall” on page 93](#)
4. [“UEBA : Executive only asset accessed by non-executive user from external network” on page 88](#)
5. [“UEBA : Detected Activity from a Locked Machine” on page 87](#)
6. [“UEBA : Bruteforce Authentication Attempts” on page 86](#)
7. [“UEBA : High Risk User Access to Critical Asset” on page 89](#)
8. [“UEBA : Multiple VPN Accounts Logged In From Single IP” on page 92](#)
9. [“UEBA : Multiple VPN Accounts Failed Login From Single IP” on page 91](#)
10. [“UEBA : Executive only asset accessed by non-executive user from internal network” on page 88](#)
11. [“UEBA : User Attempt to Use Disabled Account” on page 131](#)
12. [“UEBA : Dormant Account Use Attempted” on page 119](#)
13. [“UEBA : Expired Account Used” on page 121](#)
14. [“UEBA : Suspicious Privileged Activity \(First Observed Privilege Use\)” on page 126](#)
15. [“UEBA : Suspicious Privileged Activity \(Rarely Used Privilege\)” on page 128](#)
16. [“UEBA : User Attempt to Use a Suspended Account” on page 132](#)
17. [“UEBA : Large Outbound Transfer by High Risk User” on page 195](#)
18. [“UEBA : Multiple Blocked File Transfers Followed by a File Transfer” on page 196](#)
19. [“UEBA : Suspicious Access Followed by Data Exfiltration” on page 199](#)
20. [“UEBA : Data Exfiltration by Print” on page 192](#)
21. [“UEBA : Initial Access Followed by Suspicious Activity” on page 194](#)
22. [“UEBA : Potentially Compromised Account” on page 198](#)

23. ["UEBA : Multiple blocked file uploads followed by a successful upload" on page 198](#)
24. ["UEBA : User Potentially Phished" on page 201](#)
25. ["UEBA : Suspicious Activity Followed by Exfiltration" on page 200](#)
26. ["UEBA : Data Loss Possible" on page 193](#)
27. ["UEBA : Data Exfiltration by Removable Media" on page 192](#)
28. ["UEBA : Data Exfiltration by Cloud Services" on page 191](#)
29. ["UEBA : Repeat Unauthorized Access" on page 94](#)
30. ["UEBA : User Access - Failed Access to Critical Assets" on page 97](#)
31. ["UEBA : Unix/Linux System Accessed With Service or Machine Account" on page 97](#)
32. [Critical Systems Users Seen Update](#)
33. ["UEBA : User Accessing Account from Anonymous Source" on page 104](#)
34. ["UEBA : User Access at Unusual Times" on page 106](#)
35. ["UEBA : User Access to Internal Server From Jump Server " on page 102](#)
36. [Populate Multiple VPN Accounts Failed Login From Single IP](#)
37. ["UEBA : First Access to Critical Assets" on page 99](#)
38. ["UEBA : First Privilege Escalation" on page 123](#)
39. ["UEBA : User Account Created and Deleted in a Short Period of Time" on page 116](#)
40. ["UEBA : Account or Group or Privileges Modified" on page 111](#)
41. ["UEBA : Browsed to Pornography Website" on page 152](#)
42. ["UEBA : Browsed to Uncategorized Website" on page 159](#)
43. ["UEBA : Browsed to LifeStyle Website" on page 146](#)
44. ["UEBA : Browsed to Gambling Website" on page 140](#)
45. ["UEBA : Anonymous User Accessed a Resource" on page 162](#)
46. ["UEBA : Inbox Set to Forward to External Inbox" on page 164](#)
47. ["UEBA : TGT Ticket Used by Multiple Hosts" on page 174](#)
48. ["UEBA : Kerberos Account Enumeration Detected" on page 168](#)
49. ["UEBA : Detect Persistent SSH session" on page 176](#)
50. ["UEBA : Restricted Program Usage" on page 187](#)
51. ["UEBA : Detect Insecure Or Non-Standard Protocol" on page 175](#)
52. ["UEBA : Ransomware Behavior Detected" on page 186](#)
53. ["UEBA : User Access from Restricted Location" on page 210](#)
54. ["UEBA : User Access from Prohibited Location" on page 208](#)
55. ["UEBA : User Geography Change" on page 212](#)
56. ["UEBA : D/DoS Attack Detected" on page 221](#)
57. ["UEBA : Honeytoken Activity" on page 222](#)
58. ["UEBA : User Accessing Risky IP Anonymization" on page 229](#)
59. ["UEBA : User Accessing Risky IP Malware" on page 231](#)
60. ["UEBA : User Accessing Risky IP Spam" on page 232](#)
61. ["UEBA : Detect IOCs for WannaCry" on page 228](#)
62. ["UEBA : User Accessing Risky IP Dynamic" on page 231](#)

Access and authentication

UEBA : Bruteforce Authentication Attempts

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Bruteforce Authentication Attempts

Enabled by default

False

Default senseValue

5

Default senseValueSource

5

Description

Detects authentication failure brute force attack (Horizontal and Vertical).

Support rules

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Failures
- BB:UBA : Detecting Authentication Bruteforce Attempts (Horizontal)
- BB:UBA : Detecting Authentication Bruteforce Attempts (Vertical)

Log source types

3Com 8800 Series Switch, APC UPS, AhnLab Policy Center APC, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Bluemix Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CRE System, CRYPTOCARD CRYPTOSHIELD, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco FireSIGHT Management Center, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, CyberGuard TSP Firewall/VPN, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry FastIron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM Guardium, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access

Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Illumio Adaptive Security Platform, Imperva SecureSphere, Infoblox NIOS, Itron Smart Meter, Juniper Junos OS Platform, Juniper Junos WebApp Secure, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Lieberman Random Password Manager, LightCyber Magna, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft SCOM, Microsoft SQL Server, Microsoft SharePoint, Microsoft Windows Security Event Log, Motorola SymbolAP, Netskope Active, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, Okta, Open LDAP Software, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Monitoring, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend Micro Deep Discovery Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, Venustech Venusense Security Platform, Vormetric Data Security, WatchGuard Firewall OS, genua genugate, iT-CUBE agileSI

UEBA : Detected Activity from a Locked Machine

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Detected Activity from a Locked Machine

Enabled by default

False

Default senseValue

10

Default senseValueSource

10

Description

Detects activity from a locked machine.

Support rules

BB:UBA : Common Event Filters

BB:UBA : Windows Process Created

BB:UBA : Workstation Locked

BB:UBA : Workstation Unlocked

Log source types

Microsoft Windows Security Event Log (EventID: 4688, 4800, 4801)

UEBA : Executive only asset accessed by non-executive user from external network

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Executive only asset accessed by non-executive user from external network

Enabled by default

False

Default senseValue

15

Default senseValueSource

15

Default senseValueDestination

15

Description

Detects when a non-executive user from an external network logs on to an asset that is for executive use. Two empty reference sets will be imported with this rule: "UBA : Executive Users" and "UBA : Executive Assets". Edit the reference sets to add or remove any accounts and IP addresses that are flagged from your environment. Enable this rule after configuring the reference sets.

Support rules

BB:UBA : Common Event Filters

Required configuration

Add the appropriate values to the following reference sets: "UBA : Executive Users" and "UBA : Executive Assets". Ensure the following custom property is defined: Logon Type (custom).

Log source types

Microsoft Windows Security Event Logs (EventID: 4624)

UEBA : Executive only asset accessed by non-executive user from internal network

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Executive only asset accessed by non-executive user from internal network (formerly called UBA : Executive Only Asset Accessed by Non-Executive User)

Enabled by default

False

Default senseValue

15

Default senseValueSource

15

Default senseValueDestination

15

Description

Detects when a non-executive user logs on to an asset that is for executive use only. Two empty reference sets will be imported with this rule : "UBA : Executive Users" and "UBA : Executive Assets". Edit the reference sets to add or remove any accounts and IP addresses that are flagged from your environment. Enable this rule after configuring the reference sets.

Support rules

BB:UBA : Common Event Filters

Required configuration

- Add the appropriate values to the following reference set: "UBA : Executive Users" and "UBA : Executive Assets".
- Ensure the following custom property is defined: Logon Type

Log source types

Microsoft Windows Security Event Logs (EventID: 4624)

UEBA : High Risk User Access to Critical Asset

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : High Risk User Access to Critical Asset

Enabled by default

False

Default senseValue

15

Default senseValueSource

5

Default senseValueDestination

15

Description

Detects when a user involved in incidents (offenses) access to critical asset.

Support rules

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Success

Required configuration

Add the appropriate values to the following reference set: "Critical Assets".

Log source types

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOSHield, Carbon Black Protection, Centrifry Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, MetaInfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDoS Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor,

STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasy's Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UEBA : Large number of denied access events towards external domain

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Large number of denied access events towards external domain

Enabled by default

False

Default senseValue

10

Default senseValueSource

10

Description

Detects when there are abnormal number of denied access events towards any external domain.

Support rules

BB:UBA : Common Log Source Filters

Required configuration

Enable Search assets for username, when username is not available for event or flow data in **Admin Settings > UBA Settings**.

Log source types

Access.Access Denied, Access.ACL Deny, Access.Firewall Deny, Access.IPS Deny

UEBA : Multiple VPN Accounts Failed Login From Single IP

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Multiple VPN Accounts Failed Login From Single IP

Enabled by default

False

Default senseValue

5

Default senseValueSource

5

Default senseValueDestination

10f

Description

Detects any VPN account login failures from the "UEBA : Multiple VPN Accounts Failed Login From Single IP" reference set.

Support rules

- UEBA : Populate Multiple VPN Accounts Failed Login From Single IP
- BB:UBA : VPN Login Failed

Required configuration

Enable the following rule: "UEBA : Populate Multiple VPN Accounts Failed Login From Single IP"

Log source types

Cisco Adaptive Security Appliance (ASA)

UEBA : Multiple VPN Accounts Logged In From Single IP

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Multiple VPN Accounts Logged In From Single IP

Enabled by default

False

Default senseValue

15

Default senseValueSource

15

Description

Maps multiple VPN users that are coming from the same IP address and then raises the risk score. When the rule detects VPN users coming from the same IP address, the IP address is added to the "UBA : Multiple VPN Accounts Logged In From Single IP". Before enabling this rule, make sure the rule "UBA : Populate Multiple VPN Accounts Logged In From Single IP" is enabled and the "UBA : Multiple VPN Accounts Logged In From Single IP" reference set has data.

Support rules

- UBA : Populate Multiple VPN Accounts Logged In from Single IP
- BB:UBA : VPN Login Successful

Required configuration

Enable the following rule: "UBA : Populate Multiple VPN Accounts Logged In from Single IP"

Log source types

Cisco Adaptive Security Appliance (ASA)

UEBA : Remote access hole in corporate firewall

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Remote access hole in corporate firewall

Enabled by default

False

Default senseValue

10

Default senseValueSource

10

Description

Detects when there is a remote access hole in the firewall created by GotoMyPC and OpenVPN applications.

Support rules

- BB:UBA : GoToMyPC and OpenVPN ports
- BB:UBA : Gotomypc Process Creation and Openvpn File Creation
- BB:UBA : Common Log Source Filters

Required configuration

Ensure the following custom property is defined: Filename and Process Commandline

Note: Process Commandline matches: g2tray\.exe or Filename matches .*\.ovpn over ports 8200, 1194 or 943

Enable Search assets for username, when username is not available for event or flow data in **Admin Settings > UBA Settings**.

Log source types

Microsoft Windows Security Event Logon

UEBA : Repeat Unauthorized Access

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Repeat Unauthorized Access

Enabled by default

False

Default senseValue

10

Default senseValueSource

10

Default senseValueDestination

15

Description

Indicates that repeat unauthorized access activities were found.

Support rule

UBA : Unauthorized Access

Required configuration

Enable the following rule: "UBA : Unauthorized Access"

Log source types

Akamai KONA, Amazon AWS CloudTrail, Application Security DbProtect, Arbor Networks Pravail, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Blue Coat Web Security Service, BlueCat Networks Adonis, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CRE System, Carbon Black Protection, Centrifify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco Nexus, Cisco PIX Firewall, Cisco Wireless Services Module (WiSM), Citrix NetScaler, Configurable Firewall Filter, CorreLog Agent for IBM zOS, Custom Rule Engine, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Epic SIEM, Event CRE Injected, Extreme Dragon Network IPS, Extreme Stackable and Standalone Switches, F5 Networks BIG-IP AFM, F5 Networks BIG-IP ASM, Fidelis XPS, Flow Classification Engine, Forcepoint V Series, Fortinet FortiGate Security Gateway, Foundry Fastiron, H3C Comware Platform, HP Network Automation, HP Tandem, Honeycomb Lexicon File Integrity Monitor, Huawei S Series Switch, HyTrust CloudControl, IBM AIX® Server, IBM DB2®, IBM DataPower®, IBM Fiberlink® MaaS360®, IBM Guardium®, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM Resource Access Control Facility (RACF®), IBM Security® Access Manager for Mobile, IBM Security Identity Manager, IBM Security Network IPS (GX), IBM Tivoli® Access Manager for e-business, IBM WebSphere® Application Server, IBM i, IBM z/OS®, IBM zSecure Alert, ISC BIND, Illumio Adaptive Security Platform, Imperva Incapsula, Imperva SecureSphere, Juniper Junos OS Platform, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security

Manager, Juniper WirelessLAN, Juniper vGW, Kaspersky Security Center, Kisco Information Systems SafeNet/i, Lieberman Random Password Manager, Linux DHCP Server, Linux OS, Linux iptables Firewall, Mac OS X, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee Web Gateway, McAfee ePolicy Orchestrator, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SQL Server, Microsoft Windows Security Event Log, NCC Group DDos Secure, Nortel Contivity VPN Switch, Nortel Multiprotocol Router, Nortel VPN Gateway, OS Services Qidmap, OSSEC, Okta, Open LDAP Software, OpenBSD OS, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Palo Alto PA Series, PostFix MailTransferAgent, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, Solaris Operating System Authentication Messages, Solaris Operating System DHCP Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Sophos Enterprise Console, Sophos Web Security Appliance, Squid Web Proxy, Stonesoft Management Center, Sun ONE LDAP, Symantec Critical System Protection, Symantec Endpoint Protection, Symantec Gateway Security (SGS) Appliance, Symantec System Center, Symark Power® Broker, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend InterScan VirusWall, Trend Micro Deep Security, Universal DSM, Venustech Venusense Security Platform, Vormetric Data Security, WatchGuard Fireware OS, Zscaler Nss, genua genugate, iT-CUBE agileSI

UBA : Terminated User Activity

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Terminated User Activity

Enabled by default

False

Default senseValue

25

Description

Detects activity from any user that is listed as terminated or resigned.

Required configuration

Add the appropriate values to the following reference sets: "UBA : Terminated Users".

Note: This rule does not ignore any log sources.

Log source types

Any log source that provides a username.

UBA : Unauthorized Access

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Unauthorized Access

Enabled by default

True

Default senseValue

10

Description

Indicates that unauthorized access activities were found.

Support rules

- BB:UBA : Common Event Filters
- BB:UBA : Access Denies
- BB:UBA : Application Denies

Log source types

Akamai KONA, Amazon AWS CloudTrail, Application Security DbProtect, Arbor Networks Pravail, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Blue Coat Web Security Service, BlueCat Networks Adonis, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CRE System, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco Nexus, Cisco PIX Firewall, Cisco Wireless Services Module (WiSM), Citrix NetScaler, Configurable Firewall Filter, CorreLog Agent for IBM zOS, Custom Rule Engine, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Epic SIEM, Event CRE Injected, Extreme Dragon Network IPS, Extreme Stackable and Standalone Switches, F5 Networks BIG-IP AFM, F5 Networks BIG-IP ASM, Fidelis XPS, Flow Classification Engine, Forcepoint V Series, Fortinet FortiGate Security Gateway, Foundry Fastiron, H3C Comware Platform, HP Network Automation, HP Tandem, Honeycomb Lexicon File Integrity Monitor, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Server, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM Guardium, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Mobile, IBM Security Identity Manager, IBM Security Network IPS (GX), IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Illumio Adaptive Security Platform, Imperva Incapsula, Imperva SecureSphere, Juniper Junos OS Platform, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper WirelessLAN, Juniper vGW, Kaspersky Security Center, Kisco Information Systems SafeNet/i, Lieberman Random Password Manager, Linux DHCP Server, Linux OS, Linux iptables Firewall, Mac OS X, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee Web Gateway, McAfee ePolicy Orchestrator, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SQL Server, Microsoft Windows Security Event Log, NCC Group DDoS Secure, Nortel Contivity VPN Switch, Nortel Multiprotocol Router, Nortel VPN Gateway, OS Services Qidmap, OSSEC, Okta, Open LDAP Software, OpenBSD OS, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Palo Alto PA Series, PostFix MailTransferAgent, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, Solaris Operating System Authentication Messages, Solaris Operating System DHCP Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Sophos Enterprise Console, Sophos Web Security Appliance, Squid Web Proxy, Stonesoft Management Center, Sun ONE LDAP, Symantec Critical System Protection, Symantec Endpoint Protection, Symantec Gateway Security (SGS) Appliance, Symantec System Center, Symark Power Broker, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend InterScan VirusWall, Trend Micro Deep Security, Universal DSM, Venustech Venusense Security Platform, Vormetric Data Security, WatchGuard Fireware OS, Zscaler Nss, genua genuagate, iT-CUBE agileSI

UEBA : Unix/Linux System Accessed With Service or Machine Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Unix/Linux System Accessed With Service or Machine Account

Enabled by default

False

Default senseValue

15

Default senseValueSource

10

Default senseValueDestination

10

Description

Detects any interactive session (through GUI and CLI, both local and remote login) that is initiated by a service or machine account in UNIX and Linux servers. Accounts and allowed interactive sessions are listed in the UBA : Service, Machine Account and the UBA : Allowed Interaction Session reference sets. Edit the reference sets to add or remove any interactive session that you want to flag from your environment.

Support rules

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Firewall or ACL Accept
- BB:CategoryDefinition: Authentication Success

Required configuration

Add the appropriate values to the following reference sets: "UBA : Service, Machine Account" and "UBA : Allowed Interactive Session".

Log source types

Linux OS

UEBA : User Access - Failed Access to Critical Assets

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Access - Failed Access to Critical Assets

Enabled by default

False

Default senseValue

5

Default senseValueSource

5

Default senseValueDestination

10

Description

This rule detects authentication failures for systems located in the Critical Assets reference set.

Support Rules

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Failures

Required configuration

Add the appropriate values to the following reference set: "Critical Assets".

Log source types

3Com 8800 Series Switch, APC UPS, AhnLab Policy Center APC, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Bluemix Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CRE System, CRYPTOCARD CRYPTOSHIELD, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco FireSIGHT Management Center, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, CyberGuard TSP Firewall/VPN, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry FastIron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM Guardium, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud® Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Illumio Adaptive Security Platform, Imperva SecureSphere, Infoblox NIOS, Itron Smart Meter, Juniper Junos OS Platform, Juniper Junos WebApp Secure, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Lieberman Random Password Manager, LightCyber Magna, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield

Network IPS Appliance, McAfee ePolicy Orchestrator, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft SCOM, Microsoft SQL Server, Microsoft SharePoint, Microsoft Windows Security Event Log, Motorola SymbolAP, Netskope Active, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, Okta, Open LDAP Software, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Monitoring, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend Micro Deep Discovery Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, Venustech Venusense Security Platform, Vormetric Data Security, WatchGuard Firewall OS, genua genugate, iT-CUBE agileSI

UEBA : First Access to Critical Assets

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

Supports:

- UEBA : First Access to Critical Assets
- UEBA : Critical Systems Users Seen Update

Enabled by default

False

Default senseValue

10

Default senseValueSource

10

Description

UEBA : User Access First Access to Critical Assets: Indicates that this is the first time the user accessed a critical asset. The "Critical Systems Users Seen" reference collection governs the time-to-live of an observation. By default this rule detects the first access in three months.

UEBA : Critical Systems Users Seen Update: Updates the last seen value in the "Critical Systems Users Seen" reference collection for Destination IP/Username matches that already exist.

Support rules

- BB:CategoryDefinition: Authentication Success
- BB:UBA : Common Event Filters

Required configuration

Add the appropriate values to the following reference set: "Critical Assets".

Log source types

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOSHield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, MetaInfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasy's Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA : User Access from Multiple Hosts

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : UBA : User Access from Multiple Hosts

Enabled by default

False

Default senseValue

5

Description

Detects when a single user logs in from more than an allowed number of devices.

Support rule

BB:UBA : Common Event Filters

Log source types

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCARD CRYPTOSHIELD, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft

Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UEBA : User Access to Internal Server From Jump Server

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Access to Internal Server From Jump Server

Enabled by default

False

Default senseValue

10

Default senseValueSource

5

Default senseValueDestination

5

Description

Detects when a user uses a jump server to access the VPN or internal servers.

Support Rules

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Success

Required configuration

Add the appropriate values to the following reference sets: "UBA : Jump Servers" and "UBA : Internal Servers".

Log source types

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCARD CRYPTOSHIELD, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, MetaInfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasy's Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA : Login Anomaly

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Login Anomaly

Enabled by default

False

Default senseValue

5

Description

Indicates a sequence of login failures on a local asset. The rule might also indicate an account compromise or lateral movement activity. Ensure that the Multiple Login Failures for Single Username rule is enabled. Adjust the match and time duration parameters for this rule to tune the responsiveness.

Support rules

- BB:UBA : Common Event Filters
- Multiple Login Failures for Single Username

Required configuration

Enable the following rule: "Multiple Login Failures for Single Username"

Log source types

All supported log sources.

UEBA : User Accessing Account from Anonymous Source

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Accessing Account from Anonymous Source

Enabled by default

False

Default senseValue

15

Default senseValueSource

15

Default senseValueDestination

10

Description

Indicates that a user is accessing internal resources from an anonymous source such as TOR or a VPN.

Support Rules

- BB:CategoryDefinition: Authentication Success
- BB:UBA : Common Event Filters

Required Configuration

Set "Enable X-Force® Threat Intelligence Feed" to Yes in **Admin Settings > System Settings**.

Log source types

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOSHield, Carbon Black Protection, Centrifry Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDoS Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor,

STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UEBA : User Access at Unusual Times

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Access at Unusual Times

Enabled by default

False

Default senseValue

5

Default senseValueSource

10

Description

Indicates that users are successfully authenticating at times that are unusual for your network, as defined by "UBA: Unusual Times, %" building blocks.

Support rules

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Success
- BB:UBA : Unusual Times, Evening
- BB:UBA : Unusual Times, Overnight

Log source types

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCARD CRYPTOSHIELD, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1

Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDoS Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasy's Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA : VPN Access By Service or Machine Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : VPN Access By Service or Machine Account

Enabled by default

False

Default senseValue

10

Description

Detects when a Cisco VPN is accessed by a service or machine account. Accounts are listed in the 'UBA : Service, Machine Account' reference set. Edit this list to add or remove any accounts to flag from your environment.

Support rule

BB:UBA : VPN Mapping (logic)

Required configuration

Add the appropriate values to the following reference sets: "UBA : Service, Machine Account".

Log source types

Cisco Adaptive Security Appliance (ASA)

UBA : VPN Certificate Sharing

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : VPN Certificate Sharing

Enabled by default

False

Note: If you plan to use the UBA : VPN Certificate Sharing rule, you must update the Cisco Firewall DSM to the following:

- For V7.3.1 and later: `DSM-CiscoFirewallDevices-7.3-20170619132427.noarch.rpm`

Default senseValue

15

Description

This rule detects when a VPN event's Username is not equal to 'VPNSubjectcn'. This could indicate that there is VPN certificate sharing occurring. Certificate sharing or other authentication token sharing can make it difficult to identify who's done what. This can complicate taking next steps in the event of a compromise.

Support rules

- BB:UBA : VPN Mapping (logic)
- UBA : Subject_CN and Username Map Update
- UBA : Subject_CN and Username Mapping

These rules update the associated reference sets with the required data.

Required configuration

Enable the following rules:

- UBA : Subject_CN and Username Map Update
- UBA : Subject_CN and Username Mapping

Log source types

Cisco Adaptive Security Appliance (ASA)

UBA : Windows Access with Service or Machine Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Windows Access with Service or Machine Account

Enabled by default

False

Default senseValue

15

Description

Detects any interactive session (RDP, local login) that is initiated by a service or machine account in Windows Server. Accounts are listed in the UBA : Service, Machine Account reference set. Edit the list to add or remove any accounts to flag from your environment.

Support rules

BB:UBA : Common Event Filters

Required configuration

Add the appropriate values to the following reference sets: "UBA : Service, Machine Account".

Log source types

Microsoft Windows Security Event Log (EventID: 4776)

Accounts and privileges

UBA : Account or Group or Privileges Added

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Account or Group or Privileges Added (formerly called UBA : Account, Group or Privileges Added or Modified)

Enabled by default

False

Default senseValue

5

Description

Detects events that a user performs and that fit into one of the following categories. The rule dispatches an IBM Sense event to increment the originating user's risk score.

- Authentication.Group Added
- Authentication.Group Changed

- Authentication.Group Member Added
- Authentication.Computer Account Added
- Authentication.Computer Account Changed
- Authentication.Policy Added
- Authentication.Policy Change
- Authentication.Trusted Domain Added
- Authentication.User Account Added
- Authentication.User Account Changed
- Authentication.User Right Assigned

Note: To tune the impact of this rule on users' overall risk scores, consider modifying the building block rule "CategoryDefinition: Authentication User or Group Added or Changed" by adding event categories of interest to your organization.

Support rules

- BB:UBA : Common Event Filters
- BB:UBA : Authentication User or Group or Policy Added

Log source types

Akamai KONA, Amazon AWS CloudTrail, Application Security DbProtect, Arbor Networks Pravail, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Blue Coat Web Security Service, BlueCat Networks Adonis, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CRE System, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco Nexus, Cisco PIX Firewall, Cisco Wireless Services Module (WiSM), Citrix NetScaler, Configurable Firewall Filter, CorreLog Agent for IBM zOS, Custom Rule Engine, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Epic SIEM, Event CRE Injected, Extreme Dragon Network IPS, Extreme Stackable and Standalone Switches, F5 Networks BIG-IP AFM, F5 Networks BIG-IP ASM, Fidelis XPS, Flow Classification Engine, Forcepoint V Series, Fortinet FortiGate Security Gateway, Foundry Fastiron, H3C Comware Platform, HP Network Automation, HP Tandem, Honeycomb Lexicon File Integrity Monitor, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Server, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM Guardium, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Mobile, IBM Security Identity Manager, IBM Security Network IPS (GX), IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Illumio Adaptive Security Platform, Imperva Incapsula, Imperva SecureSphere, Juniper Junos OS Platform, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper WirelessLAN, Juniper vGW, Kaspersky Security Center, Kisco Information Systems SafeNet/i, Lieberman Random Password Manager, Linux DHCP Server, Linux OS, Linux iptables Firewall, Mac OS X, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee Web Gateway, McAfee ePolicy Orchestrator, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SQL Server, Microsoft Windows Security Event Log, NCC Group DDoS Secure, Nortel Contivity VPN Switch, Nortel Multiprotocol Router, Nortel VPN Gateway, OS Services Qidmap, OSSEC, Okta, Open LDAP Software, OpenBSD OS, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Palo Alto PA Series, PostFix MailTransferAgent, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, Solaris Operating System Authentication Messages, Solaris Operating System DHCP Logs, SonicWALL SonicOS,

Sophos Astaro Security Gateway, Sophos Enterprise Console, Sophos Web Security Appliance, Squid Web Proxy, Stonesoft Management Center, Sun ONE LDAP, Symantec Critical System Protection, Symantec Endpoint Protection, Symantec Gateway Security (SGS) Appliance, Symantec System Center, Symark Power Broker, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend InterScan VirusWall, Trend Micro Deep Security, Universal DSM, Venustech Venusense Security Platform, Vormetric Data Security, WatchGuard Fireware OS, Zscaler Nss, genua genugate, iT-CUBE agileSI

Related concepts

UEBA : Account or Group or Privileges Modified

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : DoS Attack by Account Deletion

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Account Created and Deleted in a Short Period of Time

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Dormant Account Used

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Dormant Account Use Attempted

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Expired Account Used

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : First Privilege Escalation

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : New Account Use Detected

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Privileged Activity (First Observed Privilege Use)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Privileged Activity (Rarely Used Privilege)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Attempt to Use Disabled Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Attempt to Use a Suspended Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Account or Group or Privileges Modified

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Account or Group or Privileges Modified (formerly called UEBA : User Account Change)

Enabled by default

False

Default senseValue

10

Default senseValueSource

10

Default senseValueDestination

10

Default senseValueSource

10

Default senseValueDestination

10

Description

Indicates when a user account was affected by an action which changes the user's effective privileges, either up or down.

False positive note: This event might misattribute modifications to an account name to the user making the changes. If you want to reduce this false positive possibility you can add the test 'and when Username equals AccountName'.

False negative note: This event might not detect all cases of account modifications for a user.

Support rules

- BB:UBA : Common Event Filters
- BB:UBA : Authentication User or Group or Policy Changed

Log source types

Microsoft Windows Security Event Log (EventID: 626, 642, 644, 1300, 1317, 625, 629, 4672, 4722, 4725, 4738, 4765, 4767, 4781, 4737, 4755)

Related concepts

UBA : Account or Group or Privileges Added

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : DoS Attack by Account Deletion

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Account Created and Deleted in a Short Period of Time

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Dormant Account Used

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Dormant Account Use Attempted

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Expired Account Used

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : First Privilege Escalation

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : New Account Use Detected

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Privileged Activity (First Observed Privilege Use)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Privileged Activity (Rarely Used Privilege)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Attempt to Use Disabled Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Attempt to Use a Suspended Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : DoS Attack by Account Deletion

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : DoS Attack by Account Deletion

Enabled by default

False

Default senseValue

10

Description

Detects DoS attack by checking the number of account deletion events against a fixed threshold within fixed time span.

Support rules

- BB:UBA : Common Event Filters
- BB:UBA : User Account Deleted

Log source types

Amazon AWS CloudTrail (EventID: DeleteUser)

Application Security DbProtect (EventID: Login revoked - Windows, Login dropped - standard, Database role - dropped, Database user revoked)

Aruba Mobility Controller (EventID: authmgr_user_del)

Box (EventID: DELETE_USER)

Brocade FabricOS (EventID: SEC-1181, SEC-3028)

CA ACF2 (EventID: ACF2-L)

Check Point (EventID: user_deleted, device_deleted, User Deleted)

Cilasoft QJRN/400 (EventID: C20020)

Cisco Adaptive Security Appliance (ASA) (EventID: %PIX|ASA-5-502102, %ASA-5-502102)

Cisco FireSIGHT Management Center (EventID: USER_REMOVED_CHANGE_EVENT)

Cisco Firewall Services Module (FWSM) (EventID: 502102)

Cisco Identity Services Engine (EventID: 86008, 86028)

Cisco NAC Appliance (EventID: CCA-1453, CCA-1502)

Cisco Nexus (EventID: SECURITYD-6-DELETE_STALE_USER_ACCOUNT)

Cisco Wireless LAN Controllers (EventID: 1.3.6.1.4.1.9.9.515.0.1)

CloudPassage Halo (EventID: Halo user deleted, Local account deleted (linux only))

CorreLog Agent for IBM zOS (EventID: RACF DELUSER: No Violations)

Custom Rule Engine (EventID: 3035, 3043)

Cyber-Ark Vault (EventID: 276)

EMC VMWare (EventID: AccountRemovedEvent)

Extreme Dragon Network IPS (EventID: HOST:LINUX:USER-DELETED, HOST:WIN:ACCOUNT-DELETED)

Extreme Matrix K/N/S Series Switch (EventID: User Deleted Event, has been deleted)

Extreme NAC (EventID: Deleted registered user)

Extreme NetsightASM (EventID: UserRemove)

Flow Classification Engine (EventID: 3035, 3043)

Forcepoint Sidewinder (EventID: passport deletion, all passports revoked)

HBGary Active Defense (EventID: DeleteUser)

HP Network Automation (EventID: User Deleted)

Huawei S Series Switch (EventID: SSH/6/DELUSER_SUCCESS)

IBM AIX Audit (EventID: USER_Remove SUCCEEDED)

IBM AIX Server (EventID: USER_Remove)

IBM DB2 (EventID: DROP_USER SUCCESS)

IBM DataPower (EventID: 0x81000136)

IBM IMS (EventID: USER DELETED)

IBM Proventia Network Intrusion Prevention System (IPS) (EventID: Delete User)

IBM Resource Access Control Facility (RACF) (EventID: 80 17.2, DELUSER_SUCCESS, 80 17.0)

IBM Security Access Manager for Enterprise Single Sign-On (EventID: REVOKE_IMS_ID, DELETE_IMS_ID)

IBM Security Directory Server (EventID: SDS Audit)

IBM Security Identity Governance (EventID: 50, 43, 70005)

IBM Security Identity Manager (EventID: Delete SUCCESS, Delete SUBMITTED, Delete Success)

IBM SmartCloud Orchestrator (EventID: user)

IBM Tivoli Access Manager for e-business (EventID: 13408 - Succeeded, 13408 Command Succeeded)

IBM i (EventID: GSL2502, M250100, DO_USRPRF, GSL2602, GSL2601, M260100, MC@0400, GSL2501)

IBM z/OS (EventID: 80 1.35)

Juniper Networks Network and Security Manager (EventID: adm24473)

Linux OS (EventID: userDel, Account Deleted, DEL_USER)

McAfee Application/Change Control (EventID: USER_ACCOUNT_DELETED)

McAfee ePolicy Orchestrator (EventID: 20793)

Microsoft ISA (EventID: user removed)

Microsoft Office 365 (EventID: Delete User-PartiallySucceeded, Delete user-success, Delete User-success, Delete user-PartiallySucceeded)

Microsoft SQL Server (EventID: 24129, DR - US, DR - SL, DR - LX, DR - AR, DR - SU, 24076, 24123, 38)

Microsoft Windows Security Event Log (EventID: 4743, 630, 1327, 647, 4726)

Netskope Active (EventID: Delete Admin, Deleted admin)

Nortel Application Switch (EventID: User Deleted)

Novell eDirectory (EventID: DELETE_ACCOUNT)

OS Services Qidmap (EventID: Account Deleted, User Deleted)

OSSEC (EventID: 18112)

Okta (EventID: core.user_group_member.user_remove, app.generic.import.details.delete_user)

Oracle Enterprise Manager (EventID: Computer Delete (successful), User Delete (successful))

Oracle RDBMS Audit Record (EventID: DROP USER-Standard:1, 53:1, 53:0, DROP USER-Standard:0, 53)

PGP Universal Server (EventID: ADMIN_DELETED_USER)

Palo Alto Endpoint Security Manager (EventID: User Deleted)

Pulse Secure Pulse Connect Secure (EventID: SYN24849, ADM20722, ADM24473, SYN24745, SYN24850)

RSA Authentication Manager (EventID: unknown, Deleted user, REMOVE_ORPHANED_PRINCIPALS, REMOTE_PRINCIPAL_DELETE, DELETE_PRINCIPAL)

SIM Audit (EventID: Configuration-UserAccount-AccountDeleted)

STEALTHbits StealthINTERCEPT (EventID: Active DirectorycomputerObject DeletedTrueFalse, Active DirectoryuserObject DeletedTrueFalse, Console user/group deleted, Console user/group deleted)

SafeNet DataSecure/KeySecure (EventID: Removed user)

Skyhigh Networks Cloud Security Platform (EventID: 10017)

Solaris BSM (EventID: delete user)

SonicWALL SonicOS (EventID: 559, 1157, 1158)

Trend Micro Deep Security (EventID: 651)

Universal DSM (EventID: Computer Account Removed, User Account Removed)

VMware vCloud Director (EventID: com/vmware/vcloud/event/user/remove, com/vmware/vcloud/event/user/delete)

Vormetric Data Security (EventID: DAO0090I)

iT-CUBE agileSI (EventID: AU8, U0)

Related concepts

UBA : Account or Group or Privileges Added

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Account or Group or Privileges Modified

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Account Created and Deleted in a Short Period of Time

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Dormant Account Used

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Dormant Account Use Attempted

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Expired Account Used

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : First Privilege Escalation

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : New Account Use Detected

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Privileged Activity (First Observed Privilege Use)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Privileged Activity (Rarely Used Privilege)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Attempt to Use Disabled Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Attempt to Use a Suspended Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Account Created and Deleted in a Short Period of Time

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Account Created and Deleted in a Short Period of Time

Enabled by default

False

Default senseValue

15

Default senseValueSource

15

Description

Detects when an user account is created and deleted in a short period of time.

Support rules

- BB:UBA : User Account Created
- BB:UBA : User Account Deleted
- BB:UBA : Common Event Filters

Log source types

Related concepts

UBA : Account or Group or Privileges Added

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Account or Group or Privileges Modified

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : DoS Attack by Account Deletion

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Dormant Account Used

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Dormant Account Use Attempted

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Expired Account Used

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : First Privilege Escalation

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : New Account Use Detected

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Privileged Activity (First Observed Privilege Use)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Privileged Activity (Rarely Used Privilege)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Attempt to Use Disabled Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Attempt to Use a Suspended Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Dormant Account Used

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Dormant Account Used

Enabled by default

True

Default senseValue

10

Default senseValueSource

10

Default senseValueDestination

10

Description

Detects the successful log in from an account that has been determined to be dormant.

For details on how accounts are determined to be dormant, see [“Dormant accounts” on page 55](#).

Support rule

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Failures

Log source types

Any supported log source that provides a username in the event.

Related concepts

[UBA : Account or Group or Privileges Added](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UEBA : Account or Group or Privileges Modified](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : DoS Attack by Account Deletion](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UEBA : User Account Created and Deleted in a Short Period of Time](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UEBA : Dormant Account Use Attempted](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Expired Account Used

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : First Privilege Escalation

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : New Account Use Detected

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Privileged Activity (First Observed Privilege Use)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Privileged Activity (Rarely Used Privilege)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Attempt to Use Disabled Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Attempt to Use a Suspended Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Dormant Account Use Attempted

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Dormant Account Use Attempted

Enabled by default

False

Default senseValue

5

Default senseValueSource

5

Description

Detects the failed log in attempt from an account that has been determined to be dormant.

For details on how accounts are determined to be dormant, see [“Dormant accounts” on page 55](#).

Support rule

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Failures

Log source types

3Com 8800 Series Switch, APC UPS, AhnLab Policy Center APC, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CRE System, CRYPTOCARD CRYPTOSHIELD, Carbon Black Protection, Centrify Identity Platform, Centrify Infrastructure Services, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco FireSIGHT Management Center, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, CyberGuard TSP Firewall/VPN, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, ESET Remote Administrator, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Matrix K/N/S Series Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, Extreme XSR Security Routers, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, Forcepoint Sidewinder, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM Bluemix Platform, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM Guardium, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Illumio Adaptive Security Platform, Imperva SecureSphere, Infoblox NIOS, Itron Smart Meter, Juniper Junos OS Platform, Juniper Junos WebApp Secure, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Lieberman Random Password Manager, LightCyber Magna, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Network Security Platform, McAfee ePolicy Orchestrator, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft SCOM, Microsoft SQL Server, Microsoft SharePoint, Microsoft Windows Security Event Log, Motorola SymbolAP, Netskope Active, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, Okta, OpenBSD OS, Open LDAP Software, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Palo Alto PA Series, Pirean Access: One, PostFix MailTransferAgent, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Monitoring, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sun ONE LDAP, Sybase ASE, Symantec Encryption Management Server, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Discovery Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, Venustech Venusense Security Platform, Vormetric Data Security, WatchGuard Firewall OS, genua genugate, iT-CUBE agileSI

Related concepts

[UBA : Account or Group or Privileges Added](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UEBA : Account or Group or Privileges Modified](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : DoS Attack by Account Deletion

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Account Created and Deleted in a Short Period of Time

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Dormant Account Used

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Expired Account Used

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : First Privilege Escalation

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : New Account Use Detected

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Privileged Activity (First Observed Privilege Use)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Privileged Activity (Rarely Used Privilege)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Attempt to Use Disabled Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Attempt to Use a Suspended Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Expired Account Used

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Expired Account Used. (formerly called UBA : Orphaned or Revoked or Suspended Account Used)

Enabled by default

False

Default senseValue

10

Default senseValueSource

10

Description

Indicates that a user attempted to log in to a disabled or an expired account on a local system. This rule might also suggest that an account was compromised.

Although not required, you can enable **Search assets for username, when username is not available for event or flow data** in **Admin Settings > UBA Settings**.

Support rules

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication to Expired Account
- BB:UBA : Expired Accounts (Kerberos)

Log source types

Extreme Dragon Network IPS (EventID: HOST:WIN:532-ACCOUNT-EXPIRED, HOST:WIN:535-PWD-EXPIRED)

Microsoft Windows Security Event Log (EventID: 532, 535, 4768, 4771, 4772, 4625, 4776)

IBM Proventia Network Intrusion Prevention System (IPS) (EventID: Failed_login-account_expired, Failed_login-password_expired, NovellEdirectoryExpiredAccounts, SolarisUseraddExpiredAccounts)

Cisco CatOS for Catalyst Switches (EventID: HA_POLICY_TIMER_EXPIRED)

Juniper Junos OS Platform (EventID: LOGIN_PASSWORD_EXPIRED)

Microsoft IAS Server (EventID: IAS_ACCOUNT_EXPIRED)

Related concepts

UBA : Account or Group or Privileges Added

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Account or Group or Privileges Modified

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : DoS Attack by Account Deletion

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Account Created and Deleted in a Short Period of Time

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Dormant Account Used

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Dormant Account Use Attempted

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : First Privilege Escalation

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : New Account Use Detected

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Privileged Activity (First Observed Privilege Use)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Privileged Activity (Rarely Used Privilege)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Attempt to Use Disabled Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Attempt to Use a Suspended Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : First Privilege Escalation

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : First Privilege Escalation

Enabled by default

False

Default senseValue

10

Default senseValueSource

10

Default senseValueDestination

5

Description

Indicates that a user executed privileged access for the first time. This reporting rule can be disabled to allow the tracking of user behaviors for baselining purposes.

Support rule

BB:UBA : Privileged User, First Time Privilege Use (logic)

Log source types

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Application Security DbProtect, Arbor Networks Pravail, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Web Application Firewall, Bit9 Security Platform, Bluemix Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA Top Secret, CRE System, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACSCisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco FireSIGHT Management Center, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Cloudera Navigator, CorreLog Agent for IBM zOS, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare,

Enterasys Matrix K/N/S Series Switch, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme NAC, Extreme NetsightASM, F5 Networks BIG-IP APM, F5 Networks BIG-IP ASM, F5 Networks BIG-IP LTM, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, H3C Comware Platform, HBGary Active Defense, HP Network Automation, Honeycomb Lexicon File Integrity Monitor, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM Guardium, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Directory Server, IBM Security Identity Governance, IBM Security Identity Manager, IBM Security Trusteer Apex Advanced Malware Protection, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper WirelessLAN, Juniper vGW, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, MetaInfo MetaIP, Microsoft DHCP Server, Microsoft Endpoint Protection, Microsoft Hyper-V, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft SharePoint, Microsoft Windows Security Event Log, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series Pirean Access: One, PostFix MailTransferAgent, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Samhain HIDS, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Critical System Protection, Symantec Endpoint Protection, Symantec System Center, System Notification, ThreatGRID Malware Threat Intelligence Platform, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend Micro Control Manager, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Discovery Inspector, Trend Micro Deep Security, Tripwire Enterprise, Universal DSM, VMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasy's Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

Related concepts

UBA : Account or Group or Privileges Added

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Account or Group or Privileges Modified

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : DoS Attack by Account Deletion

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Account Created and Deleted in a Short Period of Time

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Dormant Account Used

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Dormant Account Use Attempted

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Expired Account Used

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : New Account Use Detected

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Privileged Activity (First Observed Privilege Use)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Privileged Activity (Rarely Used Privilege)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Attempt to Use Disabled Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Attempt to Use a Suspended Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : New Account Use Detected

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : New Account Use Detected

Enabled by default

True

Default senseValue

5

Description

Provides reporting functions that indicate an account successfully used for the first time. Accounts are tracked and monitored by the UBA app.

Note: Prior to UBA V3.5.0 this rule monitored every event coming into QRadar and added any new user account seen on an event to UBA. It populated a reference set that stored all of the user accounts and compared every event to this reference set. Starting in V3.5.0 this rule now triggers when the app sends in an event indicating the account is new. All accounts are stored in the UBA database instead of a reference table. For more information on how new accounts are detected, see [“New accounts” on page 54](#).

Log source types

IBM Sense (EventID: new account use detected)

Related concepts

UBA : Account or Group or Privileges Added

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Account or Group or Privileges Modified

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : DoS Attack by Account Deletion

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Account Created and Deleted in a Short Period of Time

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Dormant Account Used

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Dormant Account Use Attempted

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Expired Account Used

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : First Privilege Escalation

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Privileged Activity (First Observed Privilege Use)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Privileged Activity (Rarely Used Privilege)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Attempt to Use Disabled Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Attempt to Use a Suspended Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Privileged Activity (First Observed Privilege Use)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Privileged Activity (First Observed Privilege Use)

Enabled by default

False

Default senseValue

5

Default senseValueSource

5

Description

Indicates that a user executed a privileged action that the user never executed before. Observations are kept in "UBA : Observed Activities by Low Level Category and Username" map-of-sets.

Support rules

- BB:UBA : Common Event Filters
- BB:UBA : Privileged Activity

Log source types

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Application Security DbProtect, Arbor Networks Pravail, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Web Application Firewall, Bit9 Security Platform, Bluemix Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA Top Secret, CRE System, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACSCisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco FireSIGHT Management Center, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Cloudera Navigator, CorreLog Agent for IBM zOS, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, Enterasys Matrix K/N/S Series Switch, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme NAC, Extreme NetsightASM, F5 Networks BIG-IP APM, F5 Networks BIG-IP ASM, F5 Networks BIG-IP LTM, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, H3C Comware Platform, HBGary Active Defense, HP Network Automation, Honeycomb Lexicon File Integrity Monitor, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM Guardium, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Directory Server, IBM Security Identity Governance, IBM Security Identity Manager, IBM Security Trusteer Apex Advanced Malware Protection, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper WirelessLAN, Juniper vGW, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Endpoint Protection, Microsoft Hyper-V, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft SharePoint, Microsoft Windows Security Event Log, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA SeriesPirean Access: One, PostFix MailTransferAgent, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Samhain HIDS, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Critical System Protection, Symantec Endpoint Protection, Symantec System Center, System Notification, ThreatGRID Malware Threat Intelligence Platform,

TippingPoint Intrusion Prevention System (IPS),TippingPoint X Series Appliances, Top Layer IPS, Trend Micro Control Manager, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Discovery Inspector, Trend Micro Deep Security, Tripwire Enterprise, Universal DSM, VMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

Related concepts

UBA : Account or Group or Privileges Added

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Account or Group or Privileges Modified

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : DoS Attack by Account Deletion

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Account Created and Deleted in a Short Period of Time

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Dormant Account Used

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Dormant Account Use Attempted

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Expired Account Used

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : First Privilege Escalation

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : New Account Use Detected

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Privileged Activity (Rarely Used Privilege)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Attempt to Use Disabled Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Attempt to Use a Suspended Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Privileged Activity (Rarely Used Privilege)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Privileged Activity (Rarely Used Privilege)

Enabled by default

False

Default senseValue

10

Default senseValueSource

10

Description

Indicates that a user executed a privileged action that the user has not executed recently. Observations are kept in "UBA : Recent Activities by Low Level Category and Username" map-of-sets. The sensitivity of this event can be modified by changing the TTL (time-to-live) of the Reference Map-of-Sets for "UBA : Recent Activities by Low Level Category and Username". Increasing the TTL reduces the sensitivity. Decreasing the TTL increases the sensitivity.

Support rules

- BB:UBA : Common Event Filters
- BB:UBA : Privileged Activity

Log source types

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Application Security DbProtect, Arbor Networks Pravail, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Web Application Firewall, Bit9 Security Platform, Bluemix Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA Top Secret, CRE System, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACSCisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco FireSIGHT Management Center, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Cloudera Navigator, CorreLog Agent for IBM zOS, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, Enterasys Matrix K/N/S Series Switch, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme NAC, Extreme NetsightASM, F5 Networks BIG-IP APM, F5 Networks BIG-IP ASM, F5 Networks BIG-IP LTM, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, H3C Comware Platform, HBGary Active Defense, HP Network Automation, Honeycomb Lexicon File Integrity Monitor, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM Guardium, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Directory Server, IBM Security Identity Governance, IBM Security Identity Manager, IBM Security Trusteer Apex Advanced Malware Protection, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper WirelessLAN, Juniper vGW, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, MetaInfo MetaIP, Microsoft DHCP Server, Microsoft Endpoint Protection, Microsoft Hyper-V, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft SharePoint, Microsoft Windows Security Event Log, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme

Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA SeriesPirean Access: One, PostFix MailTransferAgent, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Samhain HIDS, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Critical System Protection, Symantec Endpoint Protection, Symantec System Center, System Notification, ThreatGRID Malware Threat Intelligence Platform, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend Micro Control Manager, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Discovery Inspector, Trend Micro Deep Security, Tripwire Enterprise, Universal DSM, VMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

Related concepts

UBA : Account or Group or Privileges Added

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Account or Group or Privileges Modified

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : DoS Attack by Account Deletion

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Account Created and Deleted in a Short Period of Time

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Dormant Account Used

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Dormant Account Use Attempted

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Expired Account Used

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : First Privilege Escalation

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : New Account Use Detected

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Privileged Activity (First Observed Privilege Use)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Attempt to Use Disabled Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Attempt to Use a Suspended Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Attempt to Use Disabled Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Attempt to Use Disabled Account

Enabled by default

False

Default senseValue

10

Default senseValueSource

10

Description

Detects when a user tries to access the organization resources by using a disabled account.

Support rules

- BB:CategoryDefinition: Authentication to Disabled Account
- BB:UBA : Disabled Accounts (Kerberos)
- BB:UBA : Common Log Source Filters

Log source types

Extreme Dragon Network IPS (EventID: HOST:TACACS:REJECTED-USER, HOST:TACACS:REJECTED-USER2, HOST:WIN:530-FAILED-RESTRICTED, HOST:WIN:531-ACCOUNT-DISABLED, HOST:WIN:533-FAILED-NOT-ALLOWED, HOST:WIN:539-ACCOUNT-LOCKED, HOST:WIN:DIAL-IN-LOCKOUT, HOST:WU-FTP:DISABLED-ACCOUNT)

Microsoft Windows Security Event Log (EventID: 530, 531, 533, 534, 644, 1327, 644, 4769, 4771, 4773, 4625 Account Disabled, 4625 Account Expired, 4625 Logon Outside Normal Time, 4625 User Locked Out)

IBM Proventia Network Intrusion Prevention System (IPS) (EventID: Disabled Account Blank Pwd, Disabled Account User Pwd, Failed_login-account_disabled, Failed_login-account_locked_out, Failed_login-not_authorized_for_console_login, Failed_login-time_restriction_violation, Guessed Disabled Account Pwd, User_account_disabled, User_account_locked_out)

Cisco Intrusion Prevention System (IPS) (EventID: 3343)

Microsoft IAS Server (EventID: IAS_ACCOUNT_DISABLED, IAS_ACCOUNT_LOCKED_OUT, IAS_DIALIN_DISABLED, IAS_DIALIN_LOCKED_OUT)

Related concepts

[UBA : Account or Group or Privileges Added](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UEBA : Account or Group or Privileges Modified](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : DoS Attack by Account Deletion

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Account Created and Deleted in a Short Period of Time

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Dormant Account Used

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Dormant Account Use Attempted

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Expired Account Used

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : First Privilege Escalation

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : New Account Use Detected

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Privileged Activity (First Observed Privilege Use)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Privileged Activity (Rarely Used Privilege)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Attempt to Use a Suspended Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Attempt to Use a Suspended Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Attempt to Use a Suspended Account

Enabled by default

False

Default senseValue

10

Default senseValueSource

10

Description

Detects when a user tries to access the organization resources by using suspended or blocked privileges.

Although not required, you can enable **Search assets for username, when username is not available for event or flow data** in **Admin Settings > UBA Settings**.

Log source types

Cisco Intrusion Prevention System (IPS), Extreme Dragon Network IPS, IBM Proventia Network Intrusion Prevention System (IPS), Microsoft ISA, Microsoft Windows Security Event Log (EventID: 4656,4661,4673)

Related concepts

UBA : Account or Group or Privileges Added

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Account or Group or Privileges Modified

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : DoS Attack by Account Deletion

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Account Created and Deleted in a Short Period of Time

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Dormant Account Used

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Dormant Account Use Attempted

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Expired Account Used

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : First Privilege Escalation

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : New Account Use Detected

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Privileged Activity (First Observed Privilege Use)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Privileged Activity (Rarely Used Privilege)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Attempt to Use Disabled Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

Browsing behavior

UBA : Browsed to Business/Service Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Business/Service Website

Enabled by default

False

Default senseValue

5

Description

A user has accessed a URL that might indicate an elevated security or legal risk.

Support rule

BB:UBA : URL Category Filter

Log source types

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Palo Alto PA Series, Forcepoint V Series, Fortinet FortiGate Security Gateway

Related concepts

[UBA : Browsed to Communications Website](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Browsed to Education Website](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Browsed to Entertainment Website](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UEBA : Browsed to Gambling Website](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Browsed to Government Website](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Browsed to Information Technology Website](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Browsed to Job Search Website](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to LifeStyle Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Malicious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Mixed Content/Potentially Adult Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Phishing Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Pornography Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Religious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Scam/Questionable/Illegal Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Social Networking Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Uncategorized Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA: User Accessing Risky URL

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Communications Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Communications Website

Enabled by default

False

Default senseValue

5

Description

A user has accessed a URL which may indicate elevated security or legal risk.

Support rule

BB:UBA : URL Category Filter

Log source types

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Palo Alto PA Series, Forcepoint V Series, Fortinet FortiGate Security Gateway

Related concepts

UBA : Browsed to Business/Service Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Education Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Entertainment Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Gambling Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Government Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Information Technology Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Job Search Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to LifeStyle Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Malicious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Mixed Content/Potentially Adult Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Phishing Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Pornography Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Religious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Scam/Questionable/Illegal Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Social Networking Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Uncategorized Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA: User Accessing Risky URL

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Education Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Education Website

Enabled by default

False

Default senseValue

5

Description

Detected user browsing a website associated with education content.

Support rule

BB:UBA : URL Category Filter

Log source types

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Palo Alto PA Series, Forcepoint V Series, Fortinet FortiGate Security Gateway

Related concepts

UBA : Browsed to Business/Service Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Communications Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Entertainment Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Gambling Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Government Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Information Technology Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Job Search Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to LifeStyle Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Malicious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Mixed Content/Potentially Adult Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Phishing Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Pornography Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Religious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Scam/Questionable/Illegal Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Social Networking Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Uncategorized Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA: User Accessing Risky URL

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Entertainment Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Entertainment Website

Enabled by default

False

Default senseValue

5

Description

A user accessed a URL that might indicate elevated security or legal risk.

Support rule

BB:UBA : URL Category Filter

Log source types

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Palo Alto PA Series, Forcepoint V Series, Fortinet FortiGate Security Gateway

Related concepts

UBA : Browsed to Business/Service Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Communications Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Education Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Gambling Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Government Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Information Technology Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Job Search Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to LifeStyle Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Malicious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Mixed Content/Potentially Adult Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Phishing Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Pornography Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Religious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Scam/Questionable/Illegal Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Social Networking Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Uncategorized Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA: User Accessing Risky URL

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Gambling Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Gambling Website

Enabled by default

False

Default senseValue

5

Default senseValueSource

5

Default senseValueDestination

5

Description

A user accessed a URL that might indicate elevated security or legal risk.

Support rule

BB:UBA : URL Category Filter

Log source types

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Palo Alto PA Series, Forcepoint V Series, Fortinet FortiGate Security Gateway

Related concepts

UBA : Browsed to Business/Service Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Communications Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Education Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Entertainment Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Government Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Information Technology Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Job Search Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to LifeStyle Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Malicious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Mixed Content/Potentially Adult Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Phishing Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Pornography Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Religious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Scam/Questionable/Illegal Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Social Networking Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Uncategorized Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA: User Accessing Risky URL

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Government Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Government Website

Enabled by default

False

Default senseValue

5

Description

Detected user browsing a website associated with government content.

Support rule

BB:UBA : URL Category Filter

Log source types

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Palo Alto PA Series, Forcepoint V Series, Fortinet FortiGate Security Gateway

Related concepts

[UBA : Browsed to Business/Service Website](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Browsed to Communications Website](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Browsed to Education Website](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Browsed to Entertainment Website](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UEBA : Browsed to Gambling Website](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Browsed to Information Technology Website](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Browsed to Job Search Website](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UEBA : Browsed to LifeStyle Website](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Malicious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Mixed Content/Potentially Adult Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Phishing Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Pornography Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Religious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Scam/Questionable/Illegal Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Social Networking Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Uncategorized Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA: User Accessing Risky URL

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Information Technology Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Information Technology Website

Enabled by default

False

Default senseValue

5

Description

A user accessed a URL that might indicate elevated security or legal risk.

Support rule

BB:UBA : URL Category Filter

Log source types

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Palo Alto PA Series, Forcepoint V Series, Fortinet FortiGate Security Gateway

Related concepts

UBA : Browsed to Business/Service Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Communications Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Education Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Entertainment Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Gambling Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Government Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Job Search Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to LifeStyle Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Malicious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Mixed Content/Potentially Adult Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Phishing Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Pornography Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Religious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Scam/Questionable/Illegal Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Social Networking Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Uncategorized Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA: User Accessing Risky URL

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Job Search Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Job Search Website

Enabled by default

False

Default senseValue

15

Description

A user accessed a URL that might indicate elevated security or legal risk.

Support rule

BB:UBA : URL Category Filter

Log source types

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Palo Alto PA Series, Forcepoint V Series, Fortinet FortiGate Security Gateway

Related concepts

UBA : Browsed to Business/Service Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Communications Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Education Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Entertainment Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Gambling Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Government Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Information Technology Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to LifeStyle Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Malicious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Mixed Content/Potentially Adult Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Phishing Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Pornography Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Religious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Scam/Questionable/Illegal Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Social Networking Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Uncategorized Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA: User Accessing Risky URL

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to LifeStyle Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to LifeStyle Website

Enabled by default

False

Default senseValue

5

Default senseValueSource

5

Description

A user has accessed a URL that might indicate an elevated security or legal risk.

Support rule

BB:UBA : URL Category Filter

Log source types

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Palo Alto PA Series, Forcepoint V Series, Fortinet FortiGate Security Gateway

Related concepts

UBA : Browsed to Business/Service Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Communications Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Education Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Entertainment Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Gambling Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Government Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Information Technology Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Job Search Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Malicious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Mixed Content/Potentially Adult Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Phishing Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Pornography Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Religious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Scam/Questionable/Illegal Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Social Networking Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Uncategorized Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA: User Accessing Risky URL

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Malicious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Malicious Website

Enabled by default

False

Default senseValue

15

Description

A user accessed a URL that might indicate elevated security or legal risk.

Support rule

BB:UBA : URL Category Filter

Log source types

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Palo Alto PA Series, Forcepoint V Series, Fortinet FortiGate Security Gateway

Related concepts

UBA : Browsed to Business/Service Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Communications Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Education Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Entertainment Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Gambling Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Government Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Information Technology Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Job Search Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to LifeStyle Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Mixed Content/Potentially Adult Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Phishing Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Pornography Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Religious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Scam/Questionable/Illegal Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Social Networking Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Uncategorized Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA: User Accessing Risky URL

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Mixed Content/Potentially Adult Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Mixed Content/Potentially Adult Website

Enabled by default

False

Default senseValue

10

Description

A user accessed a URL that might indicate elevated security or legal risk.

Support rule

BB:UBA : URL Category Filter

Log source types

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Palo Alto PA Series, Forcepoint V Series, Fortinet FortiGate Security Gateway

Related concepts

UBA : Browsed to Business/Service Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Communications Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Education Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Entertainment Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Gambling Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Government Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Information Technology Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Job Search Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to LifeStyle Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Malicious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Phishing Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Pornography Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Religious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Scam/Questionable/Illegal Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Social Networking Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Uncategorized Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA: User Accessing Risky URL

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Phishing Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Phishing Website

Enabled by default

False

Default senseValue

15

Description

A user accessed a URL that might indicate elevated security or legal risk.

Support rule

BB:UBA : URL Category Filter

Log source types

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Palo Alto PA Series, Forcepoint V Series, Fortinet FortiGate Security Gateway

Related concepts

UBA : Browsed to Business/Service Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Communications Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Education Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Entertainment Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Gambling Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Government Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Information Technology Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Job Search Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to LifeStyle Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Malicious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Mixed Content/Potentially Adult Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Pornography Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Religious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Scam/Questionable/Illegal Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Social Networking Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Uncategorized Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA: User Accessing Risky URL

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Pornography Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Pornography Website

Enabled by default

False

Default senseValue

10

Default senseValueSource

5

Description

A user accessed a URL that might indicate elevated security or legal risk.

Support rule

BB:UBA : URL Category Filter

Log source types

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Palo Alto PA Series, Forcepoint V Series, Fortinet FortiGate Security Gateway

Related concepts

UBA : Browsed to Business/Service Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Communications Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Education Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Entertainment Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Gambling Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Government Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Information Technology Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Job Search Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to LifeStyle Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Malicious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Mixed Content/Potentially Adult Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Phishing Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Religious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Scam/Questionable/Illegal Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Social Networking Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Uncategorized Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA: User Accessing Risky URL

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Religious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Religious Website

Enabled by default

False

Default senseValue

5

Description

A user accessed a URL that is associated with religious content.

Support rule

BB:UBA : URL Category Filter

Log source types

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Palo Alto PA Series, Forcepoint V Series, Fortinet FortiGate Security Gateway

Related concepts

UBA : Browsed to Business/Service Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Communications Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Education Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Entertainment Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Gambling Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Government Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Information Technology Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Job Search Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to LifeStyle Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Malicious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Mixed Content/Potentially Adult Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Phishing Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Pornography Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Scam/Questionable/Illegal Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Social Networking Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Uncategorized Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA: User Accessing Risky URL

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Scam/Questionable/Illegal Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Scam/Questionable/Illegal Website

Enabled by default

False

Default senseValue

5

Description

A user accessed a URL that might indicate elevated security or legal risk.

Support rule

BB:UBA : URL Category Filter

Log source types

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Palo Alto PA Series, Forcepoint V Series, Fortinet FortiGate Security Gateway

Related concepts

[UBA : Browsed to Business/Service Website](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Browsed to Communications Website](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Browsed to Education Website](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Browsed to Entertainment Website](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UEBA : Browsed to Gambling Website](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Browsed to Government Website](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Browsed to Information Technology Website](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Browsed to Job Search Website](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to LifeStyle Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Malicious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Mixed Content/Potentially Adult Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Phishing Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Pornography Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Religious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Social Networking Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Uncategorized Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA: User Accessing Risky URL

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Social Networking Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Social Networking Website

Enabled by default

False

Default senseValue

15

Description

A user accessed a website that is categorized as Social Networking.

Support rules

BB:UBA : URL Category Filter

Log source types

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Palo Alto PA Series, Forcepoint V Series, Fortinet FortiGate Security Gateway

Related concepts

UBA : Browsed to Business/Service Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Communications Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Education Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Entertainment Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Gambling Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Government Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Information Technology Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Job Search Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to LifeStyle Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Malicious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Mixed Content/Potentially Adult Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Phishing Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Pornography Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Religious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Scam/Questionable/Illegal Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Uncategorized Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA: User Accessing Risky URL

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Uncategorized Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Uncategorized Website

Enabled by default

False

Default senseValue

5

Default senseValueSource

5

Description

A user accessed a URL that might indicate an elevated security or legal risk.

Support rule

BB:UBA : URL Category Filter

Log source types

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Palo Alto PA Series, Forcepoint V Series, Fortinet FortiGate Security Gateway

Related concepts

UBA : Browsed to Business/Service Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Communications Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Education Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Entertainment Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Gambling Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Government Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Information Technology Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Job Search Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to LifeStyle Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Malicious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Mixed Content/Potentially Adult Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Phishing Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Pornography Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Religious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Scam/Questionable/Illegal Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Social Networking Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA: User Accessing Risky URL

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA: User Accessing Risky URL

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA: User Accessing Risky URL (previously called X-Force Risky URL)

Enabled by default

False

Description

This rule detects when a local user is accessing questionable online content.

Support rules

- X-Force Risky URL

- BB:UBA : Common Event Filters

Required configuration

- Set **Enable X-Force Threat Intelligence Feed** to **Yes** in **Admin Settings > System Settings**.
- Enable the following rule: X-Force Risky URL.

Log source types

Juniper SRX Series Services Gateway, Microsoft ISA, Pulse Secure Pulse Connect Secure

Related concepts

UBA : Browsed to Business/Service Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Communications Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Education Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Entertainment Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Gambling Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Government Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Information Technology Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Job Search Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to LifeStyle Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Malicious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Mixed Content/Potentially Adult Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Phishing Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Pornography Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Religious Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Scam/Questionable/Illegal Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Browsed to Social Networking Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Browsed to Uncategorized Website

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

Cloud

UEBA : Anonymous User Accessed a Resource

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Anonymous User Accessed a Resource

Enabled by default

False

Default senseValue

15

Default senseValueSource

10

Default senseValueDestination

10

Description

Detects an anonymous user accessing a resource.

Support rules

BB:UBA : Common Event Filters

Log source types

Microsoft Office 365 (EventID: AnonymousLinkUsed)

UBA : AWS Console Accessed by Unauthorized User

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : AWS Console Accessed by Unauthorized User

Enabled by default

False

Default senseValue

10

Description

Detects an unauthorized attempt to access the Amazon Web Services (AWS) console by a user that is outside the authorized list in the 'AWS - Standard Users' reference set.

Support rules

BB:UBA : Common Event Filters

Required configuration

- Install the following package from the IBM Security App Exchange: [IBM QRadar Content Extension for Monitoring Amazon AWS](#).
- Add the appropriate values to the following reference set: "AWS - Standard Users"
- Configure the following log source: Amazon AWS CloudTrail

Log source types

Amazon AWS CloudTrail (EventID: ConsoleLogin)

UBA : External User Failed Mailbox Login

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : External User Failed Mailbox Login

Enabled by default

False

Default senseValue

10

Description

Detects repeated failures to log in to mailbox from an external user.

Support rules

BB:UBA : Common Event Filters

Log source types

Microsoft Office 365 (EventID: MailboxLogin-false)

UBA : Failed to Set Mailbox Audit Logging Bypass

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Failed to Set Mailbox Audit Logging Bypass

Enabled by default

False

Default senseValue

10

Description

Detects when a user failed to correctly set mailbox audit logging bypass.

Support rules

BB:UBA : Common Event Filters

Log source types

Microsoft Office 365 (EventID: Set-MailboxAuditBypassAssociation-false)

UEBA : Inbox Set to Forward to External Inbox

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Inbox Set to Forward to External Inbox

Enabled by default

False

Default senseValue

15

Default senseValueSource

10

Description

Detects if a mailbox is set to forward to a domain that is not listed in the Trust Domains reference set.

Support rules

BB:UBA : Common Event Filters

Required configuration

Add the appropriate values to the following reference sets: "UBA : Trusted Domains".

Log source types

Microsoft Office 365 (EventID: Set-Mailbox-true)

UBA : Internal User Failed Mailbox Login Followed by Success

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Internal User Failed Mailbox Login Followed by Success

Enabled by default

False

Default senseValue

5

Description

Detects several mailbox login failures before a successful login from an internal user.

Support rules

- BB:UBA : Common Event Filters
- BB:UBA : Mailbox Login Success
- BB:UBA : Multiple Mailbox Login Failed in a Short Period of Time

Log source types

Microsoft Office 365 (EventID: MailboxLogin-false & EventID: MailboxLogin-true)

UBA : Mailbox Permission Added and Deleted in a Short Period of Time

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Mailbox Permission Added and Deleted in a Short Period of Time

Enabled by default

False

Default senseValue

10

Description

Detects mailbox permissions that are added and deleted within an hour.

Support rules

- BB:UBA : Common Event Filters
- BB:UBA : Remove Mailbox Permission Succeeded
- BB:UBA : Add Mailbox Permission Succeeded

Log source types

Microsoft Office 365 (EventID: Add-MailboxPermission-true & Remove-MailboxPermission-true)

UBA : Non-Standard User Accessing AWS Resources

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Non-Standard User Accessing AWS Resources

Enabled by default

False

Default senseValue

10

Description

Detects a non-standard user who is attempting to access Amazon Web Services (AWS) resources.

Support rules

- BB:UBA : Common Event Filters
- AWS Cloud: S3 Bucket accessed by Non-Standard User

Log source types

Amazon Web Services Extension

UBA : Sharing Link Sent to Guest

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Sharing Link Sent to Guest

Enabled by default

False

Default senseValue

10

Description

Detects a sharing invitation being sent to a guest.

Support rule

BB:UBA : Common Event Filters

Log source types

Microsoft Office 365 (EventID: SharingInvitationCreated)

UBA : Sharing Policy Changed or Shared External (SharePoint/OneDrive)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Sharing Policy Changed or Shared External (SharePoint/OneDrive)

Enabled by default

False

Default senseValue

15

Description

Detects when an item's sharing policy is changed to share with a guest user.

Support rule

BB:UBA : Common Event Filters

Log source types

Microsoft Office 365 (EventID: ExternalSharingSet, SharingPolicyChanged)

UBA : User Added to a Group on SharePoint or OneDrive by Site Admin

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : User Added to a Group on SharePoint or OneDrive by Site Admin

Enabled by default

False

Default senseValue

10

Description

Detects a user being added to a group in Sharepoint or OneDrive by a System Admin.

Support rule

BB:UBA : Common Event Filters

Log source types

Microsoft Office 365 (EventID: Add member to group-success)

UBA : User Failed to be Added to Role

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : User Failed to be Added to Role

Enabled by default

False

Default senseValue

10

Description

Detects when an attempt to add a user to a role fails.

Support rule

BB:UBA : Common Event Filters

Log source types

Microsoft Office 365 (EventID: Add-RoleGroupMember-false, Update-RoleGroupMember-false)

Domain controller

UBA : DPAPI Backup Master Key Recovery Attempted

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : DPAPI Backup Master Key Recovery Attempted

Enabled by default

False

Default senseValue

10

Description

Detects when recovery is attempted for a DPAPI Master Key.

Support rule

BB:UBA : Common Event Filters

Log source types

Microsoft Windows Security Event Log (EventID: 4693)

UEBA : Kerberos Account Enumeration Detected

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Kerberos Account Enumeration Detected

Enabled by default

False

Default senseValue

10

Default senseValueSource

10

Default senseValueDestination

10

Description

Detects Kerberos account enumeration by detecting high number of user names being used to make Kerberos requests from same source IP.

Support rule

BB:UBA : Common Event Filters

Log source types

Microsoft Windows Security Event Log (EventID: 4768)

UBA : Multiple Kerberos Authentication Failures from Same User

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Multiple Kerberos Authentication Failures from Same User

Enabled by default

False

Default senseValue

15

Description

Detects multiple Kerberos authentication ticket rejections or failures.

Support rules

- BB:UBA : Common Log Source Filters
- BB:UBA : Kerberos Authentication Failures

Required configuration

Enable **Search assets for username, when username is not available for event or flow data** in **Admin Settings > UBA Settings**.

Log source types

Microsoft Windows Security Event Log (EventID: 4768, 4771)

UBA : Non-Admin Access to Domain Controller

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Non-Admin Access to Domain Controller

Enabled by default

False

Default senseValue

5

Description

Detects non-admin account access attempts to domain controller.

Support rule

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Success
- BB:CategoryDefinition: Authentication Failures

Required configuration

Add the appropriate values to the following reference sets: "UBA : Domain Controllers" and "UBA : Domain Controller Administrators"

Log source types

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOSHield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter,

Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasy's Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

UBA : Pass the Hash

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Pass the Hash

Enabled by default

False

Default senseValue

15

Description

Detects Windows logon events that are possibly generated during pass the hash exploits.

Support rule

BB:UBA : Common Event Filters

Required configuration:

Add the appropriate values to the following reference set: UBA : Trusted Domains.

Log source types

Microsoft Windows Security Event Logs (EventID: 4624)

UBA : Possible Directory Services Enumeration

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Possible Directory Services Enumeration

Enabled by default

False

Default senseValue

5

Description

Detects reconnaissance attempts to Directory Service Enumeration.

Support rule

BB:UBA : Common Event Filters

Required configuration

Add the appropriate values to the following reference set: "UBA : Domain Controller Administrators"

Log source types

Microsoft Windows Security Event Log (EventID: 4661)

UBA : Possible SMB Session Enumeration on a Domain Controller

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Possible SMB Session Enumeration on a Domain Controller

Enabled by default

False

Default senseValue

10

Description

Detects attempts at SMB enumeration against a domain controller.

Support rule

BB:UBA : Common Event Filters

Required configuration

Add the appropriate values to the following reference sets:

- UBA : Domain Controllers
- UBA : Domain Controller Administrators

Log source types

Microsoft Windows Security Event Log (EventID: 5140)

UBA : Possible TGT Forgery

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Possible TGT Forgery

Enabled by default

False

Default senseValue

15

Description

Detects Kerberos TGTs that contain Domain Name anomalies. These possibly indicate tickets that are generated by using pass the ticket exploits.

Support rule

BB:UBA : Common Event Filters

Required configuration

Add the appropriate values to the following reference sets: UBA : Trusted Domains.

Log source types

Microsoft Windows Security Event Logs (EventID: 4768)

UBA : Possible TGT PAC Forgery

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Possible TGT PAC Forgery

Enabled by default

False

Default senseValue

10

Description

Detects use of Forged PAC certificate to get a Service Ticket from Kerberos TGS.

Support rules

- BB:UBA : Common Event Filters
- BB:UBA : TCT PAC Forgery Patched Server

- BB:UBA : TCT PAC Forgery Unpatched Server

Required configuration

Add the appropriate values to the following reference set: "UBA : Domain Controller Administrators".

Log source types

Microsoft Windows Security Event Log (EventID: 4672, 4769)

UBA : Replication Request from a Non-Domain Controller

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Replication Request from a Non-Domain Controller

Enabled by default

False

Default senseValue

5

Description

Detects replication requests from an illegitimate Domain Controller

Support rules

BB:UBA : Common Event Filters

Required configuration

Add the appropriate values to the following reference set: "UBA : Domain Controller Administrators".

Log source types

Microsoft Windows Security Event Log (EventID: 4662)

UEBA : TGT Ticket Used by Multiple Hosts

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : TGT Ticket Used by Multiple Hosts

Enabled by default

False

Default senseValue

15

Default senseValueSource

10

Default senseValueDestination

5

Description

Detects Kerberos TGT ticket being used on two (or more) different computers.

Support rule

BB:UBA : Common Event Filters

UBA : Kerberos Account Mapping

This rule updates the associated reference sets with the required data.

Required configuration

Enable the following rules: "UBA : Kerberos Account Mapping"

Log source types

Microsoft Windows Security Event Log (EventID: 4768)

Endpoint

UEBA : Detect Insecure Or Non-Standard Protocol

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Detect Insecure Or Non-Standard Protocol

Enabled by default

False

Default senseValue

5

Default senseValueSource

5

Description

Detects any user that is communicating over unauthorized protocols that are regarded as insecure or non-standard protocols. Authorized protocols are listed in the UBA : Ports of Authorized Protocols reference set with default value 0, which is the port of QRadar events. Edit the UBA : Ports of Authorized Protocols reference set to flag from your environment before you enable this rule.

Support rules

- BB:UBA : Common Event Filters
- BB:UBA : Insecure Ports

Required configuration

Add the appropriate values to the following reference set: UBA : Ports Of Authorized Protocols.

Log source types

All supported log sources.

Related concepts

UEBA : Detect Persistent SSH session

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Internet Settings Modified

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Malware Activity - Registry Modified In Bulk

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Netcat Process Detection (Linux)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Netcat Process Detection (Windows)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Process Executed Outside Gold Disk Allowlist (Linux)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Process Executed Outside Gold Disk Allowlist (Windows)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Ransomware Behavior Detected

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Restricted Program Usage

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : User Installing Suspicious Application

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Volume Shadow Copy Created

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Detect Persistent SSH session

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Detect Persistent SSH session

Enabled by default

False

Default senseValue

10

Default senseValueSource

10

Default senseValueDestination

10

Description

Detects SSH sessions that are active for more than 10 hours.

Support rules

- BB:UBA : Common Event Filters
- BB:UBA : SSH Session Closed
- BB:UBA : SSH Session Opened

Required configuration

This rule requires both SSH Opened and SSH Closed events to occur for an accurate detection. If the log source that is used does not have an eventID for both events, you might receive inaccurate results. See the Data sources to determine eventIDs for the log source in use.

Log source types (SSH Opened)

Centrify Infrastructure Services (EventID: 27100, 27104)

Cisco IOS (EventID: %SSH-5-SSH2_SESSION, %SSH-SW2-5-SSH2_SESSION)

Custom Rule Engine (EventID: 18037, 3071)

Cyber-Ark Vault (EventID: 378)

Extreme XSR Security Routers (EventID: NEW_SSH_CONNECTION)

Flow Classification Engine (EventID: 3071, 18037)

Huawei S Series Switch (EventID: SSH/4/SFTP_REQ_RECORD)

HyTrust CloudControl (EventID: AUN0120, unknown)

IBM AIX Server (EventID: sshd2 connection established, ssh-server connect, ssh-server session open)

IBM DataPower (EventID: 0x8100011e, 0x810001e4, 0x810001e5)

Juniper MX Series Ethernet Services Router (EventID: SSH)

Juniper Networks AVT (EventID: SSH)

Mac OS X (EventID: OSX ssh session started)

OS Services Qidmap (EventID: Connection from, pam_open_session, pam_sm_open_session)

Solaris Operating System Authentication Messages (EventID: ssh session opened)

Universal DSM (EventID: SSH Opened, SSH Session Started)

Log source types (SSH Closed)

Aruba Mobility Controller (EventID: sshd_disconnect)

Centrify Infrastructure Services (EventID: 27102)

Cisco IOS (EventID: %SSH-5-SSH_CLOSE, %SSH-SW2-5-SSH2_CLOSE, %SSH-5-SSH2_CLOSE)

Custom Rule Engine (EventID: 3072, 18038, 18040)

Cyber-Ark Vault (EventID: 380, 381)

Flow Classification Engine (EventID: 3072, 18038, 18040)

Huawei S Series Switch (EventID: SSH/6/RECV_DISCONNECT)

IBM AIX Server (EventID: ssh-server disconnect, sshd2 connection lost, SSH Disconnect, sshd2 local disconnect, ssh-server session close)

OS Services Qidmap (EventID: Done with connection, pam_sm_close_session, pam_close_session, Did not receive identification string, Connection timed out, Received disconnect from IP, Connection closed)

Pulse Secure Pulse Connect Secure (EventID: GWE24572)

Universal DSM (EventID: SSH Terminated, SSH Session Finished, SSH Closed)

Related concepts

UEBA : Detect Insecure Or Non-Standard Protocol

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Internet Settings Modified

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Malware Activity - Registry Modified In Bulk

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Netcat Process Detection (Linux)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Netcat Process Detection (Windows)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Process Executed Outside Gold Disk Allowlist (Linux)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Process Executed Outside Gold Disk Allowlist (Windows)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Ransomware Behavior Detected

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Restricted Program Usage

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : User Installing Suspicious Application

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Volume Shadow Copy Created

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Internet Settings Modified

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Internet Settings Modified

Enabled by default

False

Default senseValue

15

Description

Detects modifications of internet settings on the system.

Support rule

BB:UBA : Common Event Filters

Log source types

Microsoft Windows Security Event Logs (EventID: 4657)

Related concepts

[UEBA : Detect Insecure Or Non-Standard Protocol](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UEBA : Detect Persistent SSH session](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Malware Activity - Registry Modified In Bulk](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Netcat Process Detection \(Linux\)](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Netcat Process Detection \(Windows\)](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Process Executed Outside Gold Disk Allowlist \(Linux\)](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Process Executed Outside Gold Disk Allowlist \(Windows\)](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UEBA : Ransomware Behavior Detected](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Restricted Program Usage

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : User Installing Suspicious Application

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Volume Shadow Copy Created

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Malware Activity - Registry Modified In Bulk

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Malware Activity - Registry Modified In Bulk

Enabled by default

False

Default senseValue

15

Description

Detects processes that modify multiple registry values in bulk within a shorter interval.

Support rule

BB:UBA : Common Event Filters

Log source types

Microsoft Windows Security Event Logs (EventID: 4657)

Related concepts

UEBA : Detect Insecure Or Non-Standard Protocol

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Detect Persistent SSH session

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Internet Settings Modified

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Netcat Process Detection (Linux)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Netcat Process Detection (Windows)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Process Executed Outside Gold Disk Allowlist (Linux)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Process Executed Outside Gold Disk Allowlist (Windows)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Ransomware Behavior Detected

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Restricted Program Usage

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : User Installing Suspicious Application

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Volume Shadow Copy Created

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Netcat Process Detection (Linux)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Netcat Process Detection (Linux)

Enabled by default

False

Default senseValue

15

Description

Detects netcat process on a Linux system.

Support rule

BB:UBA : Common Log Source Filters

Required configuration

Enable **Search assets for username, when username is not available for event or flow data** in **Admin Settings > UBA Settings**.

Log source types

Linux OS (EventID: SYSCALL)

Related concepts

[UEBA : Detect Insecure Or Non-Standard Protocol](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Detect Persistent SSH session

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Internet Settings Modified

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Malware Activity - Registry Modified In Bulk

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Netcat Process Detection (Windows)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Process Executed Outside Gold Disk Allowlist (Linux)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Process Executed Outside Gold Disk Allowlist (Windows)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Ransomware Behavior Detected

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Restricted Program Usage

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : User Installing Suspicious Application

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Volume Shadow Copy Created

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Netcat Process Detection (Windows)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Netcat Process Detection (Windows)

Enabled by default

False

Default senseValue

15

Description

Detects Netcat process on a Windows system.

Support rule

BB:UBA : Common Event Filters

Log source types

Microsoft Windows Security Event Logs (EventID: 4688)

Related concepts

UEBA : Detect Insecure Or Non-Standard Protocol

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Detect Persistent SSH session

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Internet Settings Modified

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Malware Activity - Registry Modified In Bulk

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Netcat Process Detection (Linux)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Process Executed Outside Gold Disk Allowlist (Linux)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Process Executed Outside Gold Disk Allowlist (Windows)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Ransomware Behavior Detected

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Restricted Program Usage

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : User Installing Suspicious Application

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Volume Shadow Copy Created

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Process Executed Outside Gold Disk Allowlist (Linux)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Process Executed Outside Gold Disk Allowlist (Linux)

Enabled by default

False

Default senseValue

15

Description

Detects processes that are created on a Linux system and alerts when the process is outside of the golden disk process allowlist.

Note: The rule is disabled by default. Enable the rule only after you populate or modify the process names to be allowlisted in the reference set 'UBA : Gold Disk Process Allowlist - Linux'.

Required configuration

- Add the appropriate values to the following reference set: "UBA : Gold Disk Process Allowlist - Linux".
- Enable **Search assets for username, when username is not available for event or flow data** in **Admin Settings > UBA Settings**.

Support rule

BB:UBA : Common Log Source Filters

Log source types

Linux OS (EventID: SYSCALL)

Related concepts

[UEBA : Detect Insecure Or Non-Standard Protocol](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UEBA : Detect Persistent SSH session](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Internet Settings Modified](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Malware Activity - Registry Modified In Bulk](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Netcat Process Detection \(Linux\)](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Netcat Process Detection \(Windows\)](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Process Executed Outside Gold Disk Allowlist \(Windows\)](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UEBA : Ransomware Behavior Detected](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UEBA : Restricted Program Usage](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : User Installing Suspicious Application](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Volume Shadow Copy Created

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Process Executed Outside Gold Disk Allowlist (Windows)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Process Executed Outside Gold Disk Allowlist (Windows)

Enabled by default

False

Default senseValue

15

Description

Detects processes that are created on a Windows system and alerts when the process is outside the golden disk process allowlist.

Note: The rule is disabled by default. Enable the rule only after you populate or modify the process names to be allowlisted in the reference set 'UBA : Gold Disk Process Allowlist - Windows'.

Required configuration

Add the appropriate values to the following reference set: "UBA : Gold Disk Process Allowlist - Windows".

Log source types

Microsoft Windows Security Event Logs (EventID: 4688)

Related concepts

UEBA : Detect Insecure Or Non-Standard Protocol

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Detect Persistent SSH session

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Internet Settings Modified

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Malware Activity - Registry Modified In Bulk

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Netcat Process Detection (Linux)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Netcat Process Detection (Windows)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Process Executed Outside Gold Disk Allowlist (Linux)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Ransomware Behavior Detected

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Restricted Program Usage

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : User Installing Suspicious Application

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Volume Shadow Copy Created

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Ransomware Behavior Detected

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Ransomware Behavior Detected

Enabled by default

False

Default senseValue

15

Default senseValueSource

10

Default senseValueDestination

10

Description

Detects behavior that is typically seen during a ransomware infection.

Support rule

BB:UBA : Common Event Filters

Required configuration

Add the appropriate values to the following reference set: "UBA : Windows Common Processes".

Log source types

Microsoft Windows Security Event Logs (EventID: 4663)

Related concepts

UEBA : Detect Insecure Or Non-Standard Protocol

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Detect Persistent SSH session

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Internet Settings Modified

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Malware Activity - Registry Modified In Bulk

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Netcat Process Detection (Linux)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Netcat Process Detection (Windows)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Process Executed Outside Gold Disk Allowlist (Linux)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Process Executed Outside Gold Disk Allowlist (Windows)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Restricted Program Usage

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : User Installing Suspicious Application

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Volume Shadow Copy Created

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Restricted Program Usage

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Restricted Program Usage

Enabled by default

False

Default senseValue

5

Default senseValueSource

5

Default senseValueDestination

5

Description

Indicates that a process is created and the process name matches one of the binary names listed in the reference set "UBA : Restricted Program Filenames". This reference set is blank by default so that you can customize it. You can populate the reference set with file names that you want to monitor for risk management.

For more information about adding or removing programs for monitoring, see [“Managing restricted programs”](#) on page 53.

Support rule

BB:UBA : Common Event Filters

Required configuration

Add the appropriate values to the following reference set: "UBA : Restricted Program Filenames".

Log source types

Microsoft Windows Security Event Log

Related concepts

[UEBA : Detect Insecure Or Non-Standard Protocol](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UEBA : Detect Persistent SSH session](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Internet Settings Modified](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Malware Activity - Registry Modified In Bulk](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Netcat Process Detection \(Linux\)](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Netcat Process Detection \(Windows\)](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Process Executed Outside Gold Disk Allowlist \(Linux\)](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Process Executed Outside Gold Disk Allowlist \(Windows\)](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UEBA : Ransomware Behavior Detected](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : User Installing Suspicious Application](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Volume Shadow Copy Created

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : User Installing Suspicious Application

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

Supports the following rules:

- UBA : User Installing Suspicious Application
- UBA : Populate Authorized Applications

Enabled by default

False

Default senseValue

15

Description

Detects application installation events and then alerts when suspicious applications are seen. Note: Populate the reference set "UBA : Authorized Applications" with the application names that are authorized in the organization. Rule "UBA : Populate Authorized Applications" can be enabled for a short duration to populate this reference set.

Rule "UBA : Populate Authorized Applications" populates the reference set "UBA : Authorized Applications" with the names of applications that are installed while this rule is enabled. Note: The rule is disabled by default. Enable for a shorter duration to populate the names while users are installing applications.

Log source types

Microsoft Windows Security Event Logs

Related concepts

UEBA : Detect Insecure Or Non-Standard Protocol

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Detect Persistent SSH session

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Internet Settings Modified

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Malware Activity - Registry Modified In Bulk

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Netcat Process Detection (Linux)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Netcat Process Detection (Windows)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Process Executed Outside Gold Disk Allowlist \(Linux\)](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Process Executed Outside Gold Disk Allowlist \(Windows\)](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UEBA : Ransomware Behavior Detected](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UEBA : Restricted Program Usage](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Volume Shadow Copy Created](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Volume Shadow Copy Created

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Volume Shadow Copy Created

Enabled by default

False

Default senseValue

15

Description

Detects shadow copies that were created using vssadmin.exe or Windows Management Instrumentation Command-line (WMIC).

Support rule

BB:UBA : Common Event Filters

Log source types

Microsoft Windows Security Event Logs (EventID: 1 or 4688)

Related concepts

[UEBA : Detect Insecure Or Non-Standard Protocol](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UEBA : Detect Persistent SSH session](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Internet Settings Modified](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Malware Activity - Registry Modified In Bulk

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Netcat Process Detection (Linux)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Netcat Process Detection (Windows)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Process Executed Outside Gold Disk Allowlist (Linux)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Process Executed Outside Gold Disk Allowlist (Windows)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Ransomware Behavior Detected

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Restricted Program Usage

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : User Installing Suspicious Application

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

Exfiltration

UEBA : Data Exfiltration by Cloud Services

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Data Exfiltration by Cloud Services

Enabled by default

False

Default senseValue

5

Default senseValueSource

5

Description

Detects users that are uploading files to personal cloud services.

Support rules

- BB:UBA : Common Event Filters
- BB:UBA : File Transfer to Cloud services

Log source types

Aruba Introspect (EventID: Cloud Exfiltration)

Fortinet FortiGate Security Gateway (EventID: 16064, 35599, 35977, 35984, 36076, 36115, 36300, 36343, 36350, 36353, 36413, 38668, 38902, 38994, 39287, 39297, 39356, 39474, 39806)

UEBA : Data Exfiltration by Print

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Data Exfiltration by Print

Enabled by default

False

Default senseValue

5

Default senseValueSource

5

Description

Detects users that are sending files to print or that are using screen capture tools such as Print Screen and Snipping Tool.

Support rules

- BB:UBA : Common Event Filters
- BB:UBA : File Transfer to Print

Log source types

Universal DSM (EventID: File Print)

Verdasys Digital Guardian (EventID: Print, ADE Print Screen)

UEBA : Data Exfiltration by Removable Media

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Data Exfiltration by Removable Media

Enabled by default

False

Default senseValue

5

Default senseValueSource

5

Description

Detects users that are transferring files to removable media such as USB and CD.

Support rules

- BB:UBA : Common Event Filters
- BB:UBA : File Transfer to CD
- BB:UBA : File Transfer to USB

Log source types

Symantec Endpoint Protection (EventID: Log writing to USB drives_File_Write, Log writing to USB drives_Write File)

Verdasys Digital Guardian (EventID: CD Burn)

UEBA : Data Loss Possible

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Data Loss Possible

Enabled by default

False

Default senseValue

15

Default senseValueSource

15

Description

Detects possible data loss determined by either the data source, event category or specific events related to data loss detection and prevention.

Support rules

- BB:UBA : Data Loss Categories
- BB:UBA : Data Loss Devices
- BB:UBA : Data Loss Events

Log source types

Check Point (EventID: Detect)

Cisco Stealthwatch (EventID: 40, 45)

Forcepoint V Series (EventID: BLOCKED_BY_WEB_DLP)

Fortinet FortiGate Security Gateway (EventID: dlp passthrough, 43720)

IBM Proventia Network Intrusion Prevention System (IPS) (EventID: BsdLprSymlink,FreebsdLpdBo, HummingbirdLpdBo, MozillaSenduidIPop3Bo, BsdLpdBo)

McAfee Network Security Platform (EventID: 0x4517f400)

Netskope Active (EventID: dlp)

Pulse Secure Pulse Connect Secure (EventID: SYS24815, SYS24843, SYS24844)

Skyhigh Networks Cloud Security Platform (EventID: Anomaly, Incident, 10003, 10004, 10005, 10036)

Symantec DLP (EventID: all ids)

TippingPoint Intrusion Prevention System (IPS) (EventID: 26335,26334, 26336,27318, 27494, 27515)

Universal DSM (EventID: Data Loss Possible, Data Loss Prevention Policy Violation)

Verdasys Digital Guardian (EventID: ADE Screen Capture, Application Data Exchange, Attach Mail, CD Burn, File Archive, File Copy, File Delete, File Move, File Recycle, File Rename, File Save As, Network Transfer Download, Network Transfer Upload, Print, Print Screen, ADE Print Process)

WatchGuard Firewall OS (EventID: 1CFF0011, 1AFF002F, 1AFF0030, 1AFF0031, 1BFF0024, 1BFF0025, 1BFF0026, 1BFF0027, 1CFF0012, 1CFF0013, 1CFF0014)

UEBA : Initial Access Followed by Suspicious Activity

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Initial Access Followed by Suspicious Activity

Enabled by default

False

Default senseValue

15

Default senseValueSource

5

Description

Detects the scenario of phishing or malware activity followed by suspicious access activity within 24 hours. Note: Edit the supported building blocks to monitor any rules that are appropriate for the environment.

Support rules

BB:UBA : Compromised Account - Initial Access

- [UBA : Browsed to Malicious Website](#)
- [UBA : Browsed to Phishing Website](#)
- [UBA : Browsed to Scam/Questionable/Illegal Website](#)
- [UBA : User Accessing Risky IP, Botnet](#)
- [UBA : User Accessing Risky IP, Malware](#)

BB:UBA : Compromised Account - Execution

- [UBA : User Geography Change](#)
- [UBA : Unauthorized Access](#)
- [UBA : User Access - Failed Access to Critical Assets](#)
- [UBA : User Access Login Anomaly](#)
- [UBA : User Accessing Account from Anonymous Source](#)
- [UBA : Account or Group or Privileges Added](#)
- [UBA : Account or Group or Privileges Modified](#)
- [UBA : User Account Created and Deleted in a Short Period of Time](#)
- [UBA : Dormant Account Use Attempted](#)
- [UBA : Dormant Account Used](#)
- [UBA : User Time, Access at Unusual Times](#)
- [“UEBA : Suspicious Privileged Activity \(Rarely Used Privilege\)” on page 128](#)

Required configuration

See supported rules

Log source types

See supported rules

UEBA : Large Outbound Transfer by High Risk User

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Large Outbound Transfer by High Risk User

Enabled by default

False

Default senseValue

15

Default senseValueSource

15

Default senseValueDestination

15

Description

Detects an outbound transfer of 200,000 bytes or more by a high risk user.

Support rules

BB:UBA : Common Event Filters

Log source types

Log sources that have the CEP Bytes Sent defined.

UEBA : Multiple Blocked File Transfers Followed by a File Transfer

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Multiple Blocked File Transfers Followed by a File Transfer

Enabled by default

False

Default senseValue

10

Default senseValueSource

10

Default senseValueDestination

10

Description

Detects exfiltration by checking for file uploads that were initially blocked but were followed by a successful upload within a span of 5 minutes.

Support rules

- BB:UBA : Common Event Filters
- BB:UBA : Blocked File Transfer
- BB:UBA : Successful File Transfer

Required configuration

This rule requires both Blocked file transfers and Successful file transfers events to occur for an accurate detection. If the log source that is used does not have an eventID for both events, you might receive inaccurate results. See the Data sources to determine eventIDs for the log source in use.

Log source types (Blocked file transfers)

Cilasoft QJRN/400 (EventID: C21020)

Cisco Call Manager (EventID: %UC_DRF-3-DRFSftpFailure)

Cisco IOS (EventID: %UPDATE-3-SFTP_TRANSFER_FAIL)

Custom Rule Engine (EventID: 18014, 18071, 18187, 4032)

Extreme Stackable and Standalone Switches (EventID: FFTP request failed)

Flow Classification Engine (EventID: 4032, 18187, 18014, 18071)

Forcepoint Sidewinder (EventID: FTP Permits, denied ftp command)

IBM i (EventID: UNR0907, UNR0908, UNR2302, GSL0118, GSL0119, GSL0318, GSL0319, GSL3718, GSL3719, GSL0618, UNR0701, UNR0707, UNR0901, UNR0910, UNR2301, UNR0705, UNR0706, UNR0708, UNR0710, UNR0801, UNR0802, UNR0905, UNR0906, GSL0619)

Juniper Networks Intrusion Detection and Prevention (IDP) (EventID: TFTP:AUDIT:READ-FAILED)

Microsoft IIS (EventID: 530)

Microsoft Operations Manager (EventID: 22095)

OSSEC (EventID: 11504, 11512)

Universal DSM (EventID: FTP Action Denied, TFTP Session Denied, FTP Denied, FileTransfer Denied)

WatchGuard Firewall OS (EventID: 1CFF0002, 1CFF0006, 1CFF0007, 1CFF0009, 1CFF0001, 1CFF0019, 1CFF0000, 1CFF0003)

Log source types (Successful file transfers)

Cilasoft QJRN/400 (EventID: C21031)

Cisco FireSIGHT Management Center (EventID: FILE_EVENT, FILE_EVENT_0)

Cisco IOS (EventID: %FTPSERVER-6-NEWCONN)

Cisco IronPort (EventID: FTP_connection)

Custom Rule Engine (EventID: 18010, 4031, 18431, 18183)

DG Technology MEAS (EventID: 119-003, 119-070)

Flow Classification Engine (EventID: 18010, 4031, 18431, 18183)

Flow Device Type (EventID: 21984, 21879, 51337, 51336, 35159, 21910)

Huawei S Series Switch (EventID: FTSP/5/REQUEST)

IBM Proventia Network Intrusion Prevention System (IPS) (EventID: FTP, TFTP)

IBM i (EventID: MLD1200, MLD2100, MO10300, MO10400, MO11800, MO12100, MO12400, MO20200, MO20300, MO21300, MO21800, MO21900, GSL0101, GSL0102, GSL0301, GSL0302, GSL3701, GSL3702, MO90100, UNA0705, UNA0706, UNA0708, UNA0710, UNA0801, UNA0802, UNA0905, UNA0906, UNA0907, UNA0908, UNA2302, UNA0601, UNA0604, UNA0605, UNA0607, UNA0701, UNA0707, UNA0901, UNA0902, UNA0910, UNA2301, M030100, MLD1100)

Juniper MX Series Ethernet Services Router (EventID: TFTP, FTP)

Juniper Networks AVT (EventID: TFTP, FTP)

Microsoft IIS (EventID: 150, 125, 225)

ProFTPD Server (EventID: FTP session opened)

Solaris Operating System Authentication Messages (EventID: ftp connection)

SonicWALL SonicOS (EventID: 1112, 1113)

Squid Web Proxy (EventID: 3C0002_ALLOWED)

Trend InterScan VirusWall (EventID: Trend ftpconnect)

Universal DSM (EventID: File Transfer, FTP Opened, FTP Action Allowed, TFTP Session Opened)

Verdasys Digital Guardian (EventID: Network Transfer Upload, Network Transfer Download)

WatchGuard Firewall OS (EventID: 2AFF0004, 1CFF0019)

UEBA : Multiple blocked file uploads followed by a successful upload

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Multiple blocked file uploads followed by a successful upload

Enabled by default

False

Default senseValue

10

Default senseValueSource

10

Default senseValueDestination

10

Description

Detects when there is a high volume of blocked file uploads followed by a successful upload.

Support rules

- BB:UBA : Successful File Upload
- BB:UBA : Multiple Blocked File Uploads
- BB:UBA : Common Log Source Filters

Note: Events for both building blocks are over ports 443, 80 and 21

Required configuration

Enable Search assets for username, when username is not available for event or flow data in **Admin Settings > UBA Settings**.

Log source types

Blocked file uploads: events categories: (Access.FTP Action Denied, Access.Firewall Session Closed, Access.Access Denied)

Successful file upload: event categories: (Access.FTP Action Allowed, Access.Firewall Session Opened, Access.Access Permitted)

UEBA : Potentially Compromised Account

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Potentially Compromised Account

Enabled by default

False

Default senseValue

25

Default senseValueSource

25

Default senseValueDestination

25

Description

Detects scenario of suspicious activity followed by exfiltration within 24 hours.

Support rules

UBA : Initial Access Followed by Suspicious Activity

UBA : Suspicious Activity Followed by Exfiltration

Required configuration

See supported rules

Log source types

See supported rules

UEBA : Suspicious Access Followed by Data Exfiltration

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Access Followed by Data Exfiltration

Enabled by default

False

Default senseValue

15

Default senseValueSource

15

Default senseValueDestination

15

Description

Detects access from unusual, restricted, or prohibited locations followed by a data exfiltration attempt.

Support rule

- BB:UBA : Common Event Filters

- BB:UBA : Data Exfiltration
- UBA : User Access from Restricted Location
- UBA : User Access from Prohibited Location
- UBA : User Geography, Access from Unusual Locations

Required configuration

Enable the following rules:

- UBA : User Access from Restricted Location
- UBA : User Access from Prohibited Location
- UBA : User Geography, Access from Unusual Locations

Log source types

Cisco Stealthwatch (EventID: 45)

IBM Security Trusteer Apex Advanced Malware Protection
(EventID: ConnectionCreate.Connection_Test, CerberusNG.ent_create_remote_thread, ConnectionCreate.in_suspend_state, ConnectionCreate.orphant_thread_connect, close.file_inspection, processcreate.file_inspection)

Skyhigh Networks Cloud Security Platform (EventID: 10003, 10004)

UEBA : Suspicious Activity Followed by Exfiltration

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Suspicious Activity Followed by Exfiltration

Enabled by default

False

Default senseValue

15

Default senseValueSource

15

Default senseValueDestination

15

Description

Detects scenario of suspicious activity followed by exfiltration within 24 hours.

Support rules

BB:UBA : Compromised Account - Execution

- [“UEBA : User Geography Change” on page 212](#)
- [“UBA : Unauthorized Access” on page 95](#)
- [“UEBA : User Access - Failed Access to Critical Assets” on page 97](#)

- [“UBA : Login Anomaly” on page 104](#)
- [“UEBA : User Accessing Account from Anonymous Source” on page 104](#)
- [UBA : Account or Group or Privileges Added](#)
- [UBA : Account or Group or Privileges Modified](#)
- [UBA : User Account Created and Deleted in a Short Period of Time](#)
- [UBA : Dormant Account Use Attempted](#)
- [UBA : Dormant Account Used](#)
- [UBA : User Time, Access at Unusual Times](#)
- [“UEBA : Suspicious Privileged Activity \(Rarely Used Privilege\)” on page 128](#)

BB:UBA : Compromised Account - Exfiltration

- [“UEBA : Large Outbound Transfer by High Risk User” on page 195](#)
- [“UEBA : Suspicious Access Followed by Data Exfiltration” on page 199](#)
- [“UBA : Potential Access to DGA Domain” on page 225](#)

Required configuration

See supported rules

Log source types

See supported rules

UEBA : User Potentially Phished

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Potentially Phished

Enabled by default

False

Default senseValue

10

Default senseValueSource

5

Description

Detects 3 or more instances of potential phishing attacks on a single user within an hour. Note: Edit the supported building block to monitor any rules that are appropriate for the environment.

Support rules

BB:UBA : Compromised Account - Initial Access

- [UBA : Browsed to Malicious Website](#)
- [UBA : Browsed to Phishing Website](#)
- [UBA : Browsed to Scam/Questionable/Illegal Website](#)
- [UBA : User Accessing Risky IP, Botnet](#)

- UBA : User Accessing Risky IP, Malware

Required configuration

See supported rules

Log source types

See supported rules

Geography

UBA : Anomalous Account Created From New Location

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Anomalous Account Created From New Location

Enabled by default

False

Default senseValue

5

Description

Detects anomalous account creation activity from new location.

Support rules

- BB:UBA : Cloud Endpoints
- BB:UBA : User Account Created
- BB:UBA : Common Event Filters
- UBA : User Geography Change

Required configuration

Enable the following rule: "UBA : User Geography Change".

Log source types

AhnLab Policy Center APC (EventID: Administrator Account Add:Succeeded, ADD_ADMIN_ACCOUNT_SUCCESS)

Application Security DbProtect (EventID: Database user created, Login created - standard, Login added - Windows, Database role - created)

Aruba Mobility Controller (EventID: authmgr_user_add)

Bit9 Security Platform (EventID: User_group_created, User_group_modified, User_group_deleted, Console_user_created, Console_user_modified, Console_user_deleted)

Box (EventID: NEW_USER)

Brocade FabricOS (EventID: SEC-1180,SEC-3025, SEC-1182)

CA ACF2 (EventID: ACF2-L)

Check Point (EventID: User Added, device_added)
Cilasoft QJRN/400 (EventID: C20010, C20011)
Cisco Adaptive Security Appliance (ASA) (EventID: %PIX|ASA-5-502101, %ASA-5-502101)
Cisco Firewall Services Module (FWSM) (EventID: 502101, 504001)
Cisco IOS (EventID: %APF-6-USER_NAME_CREATED)
Cisco Identity Services Engine (EventID: 86006)
Cisco NAC Appliance (EventID: CCA-1500)
Cisco PIX Firewall (EventID: %PIX-0-502101, %PIX-1-502101, %PIX-2-502101, %PIX-3-502101, %PIX-4-502101, %PIX-5-502101, %PIX-6-502101, %PIX-7-502101)
Cisco PIX Firewall (EventID: 502101)
Cisco Wireless LAN Controllers (EventID: %APF-6-USER_NAME_CREATED, 1.3.6.1.4.1.9.9.515.0.2)
Cisco Wireless Services Module (WiSM) (EventID: %AAA-6-GUEST_ACCOUNT_CREATE, %APF-6-USER_NAME_CREATED)
CloudPassage Halo (EventID: Halo user added, Halo user re-added, Local account created (linux only))
CorreLog Agent for IBM zOS (EventID: RACF ADDUSER: No Violations)
Cyber-Ark Vault (EventID: 180, 2)
EMC VMWare (EventID: AccountCreatedEvent)
Extreme Dragon Network IPS (EventID: HOST:WIN:ACCOUNT-CREATED)
Extreme Matrix K/N/S Series Switch (EventID: created with, User Created Event)
Extreme NAC (EventID: Added registered user, Add Registered User)
Flow Classification Engine (EventID: 3031, 3041)
Forcepoint Sidewinder (EventID: passport addition)
Fortinet FortiGate Security Gateway (EventID: add, auth-logon)
Foundry Fastiron (EventID: SNMP_USER_ADDED)
HBGary Active Defense (EventID: CreateUser)
HP Network Automation (EventID: User Added)
IBM AIX Audit (EventID: USER_Create SUCCEEDED)
IBM AIX Server (EventID: USER_Create)
IBM DB2 (EventID: ADD_USER SUCCESS)
IBM IMS (EventID: USER CREATED)
IBM Resource Access Control Facility (RACF) (EventID: 80 10.0, 80 10.2)
IBM Security Access Manager for Enterprise Single Sign-On (EventID: PRE_PROVISION_IMS_USER, AA_SCR_REGISTRATION, REGISTER_MAC_IDENTITY, REGISTER_IDENTITY)
IBM Security Directory Server (EventID: SDS Audit)
IBM Security Identity Governance (EventID: 49, 70004, 42)
IBM Security Identity Manager (EventID: Add Success, Add SUBMITTED, Add SUCCESS)
IBM SmartCloud Orchestrator (EventID: user)
IBM Tivoli Access Manager for e-business (EventID: 13402 - Succeeded, 13401 - Succeeded, 13402 Command Succeeded, 13401 Command Succeeded)
IBM i (EventID: GSL2401,MC@0300, GSL2402, M240100, CP_CRT)

Imperva SecureSphere (EventID: NEW_USERS_ACCOUNT, SOX_NEW_USERS, SOX - New users, New Users Account)

Itron Smart Meter (EventID: CEUI-AUDIT-27, CEUI.AUDIT.26)

Juniper Networks Network and Security Manager (EventID: adm23303, aut20167, adm30407, aut20168, adm20716, adm20717)

Linux OS (EventID: ADD_USER)

McAfee Application/Change Control (EventID: USER_ACCOUNT_CREATED)

McAfee ePolicy Orchestrator (EventID: 20792)

Microsoft ISA (EventID: user added)

Microsoft SQL Server (EventID: CR - SU, CR - US, CR - SL, CR - LX, CR - AR, CR - WU, 24127, 24121, 24075)

Microsoft SharePoint (EventID: 37)

Microsoft Windows Security Event Log (EventID: 624, 645, 1318, 4720, 4741)

NCC Group DDos Secure (EventID: 1003)

Netskope Active (EventID: Create Admin, Created new admin)

Novell eDirectory (EventID: CREATE_ACCOUNT)

OS Services Qidmap (EventID: User Account Added)

OSSEC (EventID: 5902, 18110)

Okta (EventID: app.user_management.push_new_user_success, app.generic.import.details.add_user, app.generic.import.new_user, app.user_management.provision_user, app.user_management.push_new_user, app.user_management.push_profile_success, core.user.config.user_creation.success, core.user_group_member.user_add, cvd.user_profile_bootstrapped, cvd.appuser_profile_bootstrapped)

OpenBSD OS (EventID: add user)

Oracle Enterprise Manager (EventID: User Create (successful), Computer Create (successful))

Oracle RDBMS Audit Record (EventID: 51:1, 51:0, CREATE USER-Standard:1, CREATE USER-Standard:0)

Oracle RDBMS OS Audit Record (EventID: 51)

Pirean Access: One (EventID: IsimUserRegistration;*;1)

Pulse Secure Pulse Connect Secure (EventID: ADM23303, ADM20265, AUT20167, ADM30407, AUT20168)

RSA Authentication Manager (EventID: Added user, unknown, REMOTE_PRINCIPAL_CREATE, CREATE_PRINCIPAL, CREATE_AM_PRINCIPAL)

SIM Audit (EventID: Configuration-UserAccount-AccountAdded)

STEALTHbits StealthINTERCEPT (EventID: Active DirectorycomputerObject AddedTrueFalse, Console ? user/group added, Console [X] user/group added, Active DirectoryuserObject AddedTrueFalse, Console - user/group added)

SafeNet DataSecure/KeySecure (EventID: Added user)

Salesforce Security Auditing (EventID: Created new Customer User, Created new user)

Skyhigh Networks Cloud Security Platform (EventID: 10016)

Solaris BSM (EventID: create user)

SonicWALL SonicOS (EventID: 558)

Symantec Encryption Management Server (EventID: ADMIN_IMPORTED_USER)

ThreatGRID Malware Threat Intelligence Platform (EventID: user-account-creation)

Trend Micro Deep Discovery Email Inspector (EventID: SYSTEM_EVENT_ACCOUNT_CREATED)

Trend Micro Deep Security (EventID: 650)

Universal DSM (EventID: Computer Account Added, User Account Added)

VMware vCloud Director (EventID: com/vmware/vcloud/event/user/create, com/vmware/vcloud/event/user/import)

Vormetric Data Security (EventID: DAO0089I)

iT-CUBE agileSI (EventID: U0, AU7)

Related concepts

UBA : Anomalous Cloud Account Created From New Location

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : User Access from Multiple Locations

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Access from Prohibited Location

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Access from Restricted Location

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Geography Change

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : User Access from Unusual Locations

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Anomalous Cloud Account Created From New Location

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Anomalous Cloud Account Created From New Location

Enabled by default

False

Default senseValue

10

Description

Detects cloud account creation activities from a new location.

Support rules

- BB:UBA : Common Event Filters
- BB:UBA : Cloud Endpoints
- BB:UBA : User Account Created

- UBA : User Geography Change

Required configuration

Enable the following rule: "UBA : User Geography Change".

Log source types

Amazon AWS CloudTrail (EventID: CreateUser)

Microsoft Office 365 (EventID: Add User-success, Add user-PartiallySucceeded)

Related concepts

UBA : Anomalous Account Created From New Location

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : User Access from Multiple Locations

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Access from Prohibited Location

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Access from Restricted Location

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Geography Change

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : User Access from Unusual Locations

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : User Access from Multiple Locations

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : User Access from Multiple Locations

Enabled by default

False

Default senseValue

5

Description

Indicates that multiple locations or sources are using the same user account simultaneously. Adjust the match and duration parameters to tune responsiveness.

Support rule

BB:UBA : Common Event Filters

Log source types

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCARD CRYPTOSHIELD, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, MetaInfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasy's Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

Related concepts

[UBA : Anomalous Account Created From New Location](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Anomalous Cloud Account Created From New Location

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Access from Prohibited Location

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Access from Restricted Location

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Geography Change

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : User Access from Unusual Locations

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Access from Prohibited Location

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Access from Prohibited Location

Enabled by default

False

Default senseValue

15

Default senseValueSource

10

Description

Detects user access from a location not in the "UBA : Allowed Location List."

Support rules:

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Success

Required configuration

Add the appropriate values to the following reference set: UBA : Allowed Location List

Log source types

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA

Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOShield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasy's Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

Related concepts

[UBA : Anomalous Account Created From New Location](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Anomalous Cloud Account Created From New Location](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : User Access from Multiple Locations](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Access from Restricted Location

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Geography Change

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : User Access from Unusual Locations

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Access from Restricted Location

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Access from Restricted Location

Enabled by default

False

Default senseValue

15

Default senseValueSource

10

Default senseValueDestination

5

Description

Detects user access from a location on the "UBA : Restricted Location List." You can add countries from "geographic location" to the "UBA : Restricted Location List."

Support rules

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Success

Required configuration

Add the appropriate values to the following reference set: UBA : Restricted Location List

Log source types

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOSHield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco

ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDoS Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasy's Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

Related concepts

UBA : Anomalous Account Created From New Location

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Anomalous Cloud Account Created From New Location

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : User Access from Multiple Locations

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Access from Prohibited Location

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Geography Change

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : User Access from Unusual Locations

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Geography Change

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Geography Change

Enabled by default

False

Default senseValue

5

Default senseValueSource

10

Description

A match indicates that a user logged in remotely from a country that is different from the country of the user's last remote login. This rule might also indicate an account compromise, particularly if the rule matches occurred closely in time.

Support rules

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Success
- UEBA : User Geography Map

Required configuration

Enable the following rule: UEBA : User Geography Map

Log source types

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCARD CRYPTOSHIELD, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX

Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo,Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch,Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino,IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile,IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager,Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance,McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server,Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDoS Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series,Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit,SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM,Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasy's Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

Support rule

User Geography Map

This rule updates the associated reference sets with the required data.

Related concepts

[UBA : Anomalous Account Created From New Location](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Anomalous Cloud Account Created From New Location](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : User Access from Multiple Locations](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Access from Prohibited Location

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Access from Restricted Location

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : User Access from Unusual Locations

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : User Access from Unusual Locations

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : User Access from Unusual Locations

Enabled by default

False

Default senseValue

15

Description

Indicates that users were able to authenticate in countries that are unusual for your network, as defined by the building block rule "UBA : BB : Unusual Source Locations".

Support rules

- BB:UBA : Unusual Source Locations
- BB:CategoryDefinition: Authentication Success
- BB:UBA : Common Event Filters

Log source types

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOSHield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification

Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, MetaInfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasy's Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

Related concepts

UBA : Anomalous Account Created From New Location

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Anomalous Cloud Account Created From New Location

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : User Access from Multiple Locations

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Access from Prohibited Location

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Access from Restricted Location

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Geography Change

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

MaaS360 Security

UBA : MaaS360 detected device with low encryption level

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : MaaS360 detected device with low encryption level

Enabled by default

False

Default senseValue

5

Description

Device has been detected with a low encryption level.

Required configuration

IBM MaaS360 Security DSM and events.

Support rule

BB:UBA : Common Event Filters

Log source types

IBM MaaS360 Security (Event ID: ENCRYPTION_LEVEL with Event Category : VULNERABILITY)

UBA : MaaS360 device out of compliance due to non-roaming data usage

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : MaaS360 device out of compliance due to non-roaming data usage

Enabled by default

False

Default senseValue

5

Description

Device is not compliant because it exceeded the mobile usage limit set by MaaS Admin.

Required configuration

IBM MaaS360 Security DSM and events.

Support rule

BB:UBA : Common Event Filters

Log source types

IBM MaaS360 Security (Event ID: NON_ROAMING_DATA_USAGE with Event Category : COMPLIANCE)

UBA : MaaS360 device out of compliance due to device being rooted

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : MaaS360 device out of compliance due to device being rooted

Enabled by default

False

Default senseValue

5

Description

Device is not compliant because it was jailbroken or rooted to bypass OS restrictions.

Required configuration

IBM MaaS360 Security DSM and events.

Support rule

BB:UBA : Common Event Filters

Log source types

IBM MaaS360 Security ((Event ID: DEVICE_ROOTED with Event Category : COMPLIANCE)

UBA : MaaS360 device out of compliance due to encryption level

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : MaaS360 device out of compliance due to encryption level

Enabled by default

False

Default senseValue

5

Description

Device is not compliant because it support designated levels of encryption set by MaaS Admin.

Required configuration

IBM MaaS360 Security DSM and events.

Support rule

BB:UBA : Common Event Filters

Log source types

IBM MaaS360 Security (Event ID: ENCRYPTION_LEVEL with Event Category : COMPLIANCE)

UBA : MaaS360 device out of compliance due to OS version

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : MaaS360 device out of compliance due to OS version

Enabled by default

False

Default senseValue

5

Description

Device is not compliant because it required updated OS versions.

Required configuration

IBM MaaS360 Security DSM and events.

Support rule

BB:UBA : Common Event Filters

Log source types

IBM MaaS360 Security (Event ID: OS_VERSION with Event Category : COMPLIANCE)

UBA : MaaS360 malicious SMS received

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : MaaS360 malicious SMS received

Enabled by default

False

Default senseValue

5

Description

Detects MaaS360 event indicating a user received a malicious SMS message.

Required configuration

IBM MaaS360 Security DSM and events.

Support rule

BB:UBA : Common Event Filters

Log source types

IBM MaaS360 Security (Event ID: MALICIOUS_SMS with Event Category : THREAT)

UBA : MaaS360 malicious email received

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : MaaS360 malicious email received

Enabled by default

False

Default senseValue

5

Description

Detects MaaS360 event indicating a user received a malicious email.

Required configuration

IBM MaaS360 Security DSM and events.

Support rule

BB:UBA : Common Event Filters

Log source types

IBM MaaS360 Security ((Event ID: MALICIOUS_EMAIL with Event Category : THREAT)

UBA : MaaS360 URL access blocked

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : MaaS360 URL access blocked

Enabled by default

False

Default senseValue

10

Description

Detects MaaS360 event indicating a user's access to a URL has been blocked.

Required configuration

IBM MaaS360 Security DSM and events.

Support rule

BB:UBA : Common Event Filters

Log source types

IBM MaaS360 Security (Event ID: BLOCKED_URL_ACCESS with Event Category : COMPLIANCE)

UBA : MaaS360 malware application installed

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : MaaS360 malware application installed

Enabled by default

False

Default senseValue

15

Description

Detects MaaS360 event indicating a user has malware on their device.

Required configuration

IBM MaaS360 Security DSM and events.

Support rule

BB:UBA : Common Event Filters

Log source types

IBM MaaS360 Security (Event ID: MALWARE with Event Category : THREAT)

UBA : MaaS360 malicious URL accessed

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : MaaS360 malicious URL accessed

Enabled by default

False

Default senseValue

15

Description

Detect phishing links clicked from iOS and Android devices irrespective of the source.

Required configuration

IBM MaaS360 Security DSM and events.

Support rule

BB:UBA : Common Event Filters

Log source types

IBM MaaS360 Security (Event ID: MALICIOUS_URL with Event Category : THREAT)

Network traffic and attacks

UEBA : D/DoS Attack Detected

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : D/DoS Attack Detected

Enabled by default

False

Default senseValue

15

Default senseValueSource

10

Default senseValueDestination

15

Description

Detects network Denial of Service (DoS) attacks by a user.

Note: Before you can use this rule, complete the following steps:

1. From the **Admin** tab, click **UEBA Settings**.
2. Select the **Search assets for username, when username is not available for event or flow data** checkbox to search for user names in the asset table. The UEBA app uses assets to look up a user for an IP address when no user is listed in an event.

3. The event rule needs "Snort Open Source IDS" log source to work.

Support rules

- BB:UBA : Common Log Source Filters
- BB:CategoryDefinition: DDoS Attack Events
- BB:CategoryDefinition: Network DoS Attack
- BB:CategoryDefinition: Service DoS

Required configuration

Enable **Search assets for username, when username is not available for event or flow data** in **Admin Settings > UBA Settings**.

Log source types

Akamai KONA, Application Security DbProtect, Aruba Mobility Controller, Barracuda Web Application Firewall, Brocade FabricOS, CRE System, Check Point, Cisco Adaptive Security Appliance (ASA), Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Intrusion Prevention System (IPS), Cisco PIX Firewall, Cisco Stealthwatch, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Custom Rule Engine, CyberGuard TSP Firewall/VPN, Enterprise-IT-Security.com SF-Sherlock, Event CRE Injected, Extreme Dragon Network IPS, Extreme HiPath, F5 Networks BIG-IP AFM, F5 Networks BIG-IP ASM, F5 Networks BIG-IP LTM, Fair Warning, FireEye, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, Huawei AR Series Router, IBM Proventia Network Intrusion Prevention System (IPS), IBM Security Network IPS (GX), Imperva Incapsula, Juniper Junos OS Platform, Juniper Junos WebApp Secure, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Motorola SymbolAP, NCC Group DDoS Secure, Niksun 2005 v3.5, Nortel Application Switch, OS Services Qidmap, OSSEC, Palo Alto PA Series, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, SonicWALL SonicOS, Squid Web Proxy, Stonesoft Management Center, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), Top Layer IPS, Trend Micro Deep Security, Universal DSM, Vectra Networks Vectra, Venustech Venusense Security Platform, WatchGuard Fireware OS

Related concepts

[UEBA : Honeytoken Activity](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UBA : Network Traffic : Capture Monitoring and Analysis Program Usage](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Honeytoken Activity

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Honeytoken Activity

Enabled by default

False

Default senseValue

10

Default senseValueSource

10

Description

Detects activity using a Honeytoken account.

Support rules

BB:UBA : Common Event Filters

Required configuration

Add the appropriate values to the following reference sets: UBA : Honeytoken Accounts

Add the appropriate log sources to the following log source groups: UBA : Systems with Honeytoken Accounts.

Log source types

All log sources added to the UBA : Systems with Honeytoken Accounts log source group.

Related concepts

UEBA : D/DoS Attack Detected

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Network Traffic : Capture Monitoring and Analysis Program Usage

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Network Traffic : Capture Monitoring and Analysis Program Usage

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Network Traffic : Capture Monitoring and Analysis Program Usage

Enabled by default

False

Default senseValue

15

Description

Indicates that a process is created and the process name matches one of the binary names that are listed in the reference set "UBA : Network Capture, Monitoring and Analysis Program Filenames". This reference set lists the binary names of network packet capturing software. The reference set is pre-populated with the names of some common network protocol analysis software filenames.

For more information about adding or removing programs for monitoring, see [Managing network monitoring tools](#).

Support rule

BB:UBA : Common Event Filters

Required configuration

Add the appropriate values to the following reference set: UBA : Network Capture Monitoring and Analysis Program Filenames.

Log source types

Microsoft Windows Security Event Log

Related concepts

[UEBA : D/DoS Attack Detected](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

[UEBA : Honeytoken Activity](#)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Potential Lateral Movement

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Potential Lateral Movement

Enabled by default

True

Default senseValue

25

Description

Detection of potential lateral movement based on machine learning analysis of internal destination IP address, port, and network zone usage.

Required configuration

Install Machine Learning and enable the Lateral Movement models.

Log source types

IBM Sense (EventID: internal asset usage, internal destination port, network zones, new internal asset, new internal destination port, new network zone)

Related concepts

[“Lateral Movement : Network Zone Activity” on page 258](#)

The *Lateral Movement : Network Zone Activity* model determines if a user's network zone is significantly different from the user's defined group.

[“Lateral Movement : Internal Destination Port Activity” on page 257](#)

The *Lateral Movement : Internal Destination Port Activity* model tracks a user's activity to internal destination port activity by time and creates a model for the predicted weekly behavior patterns.

[“Lateral Movement : Internal Asset Usage” on page 256](#)

The *Lateral Movement : Internal Asset Usage* model tracks a user's internal destination asset activity by time and creates a model for the predicted weekly behavior patterns.

QRadar DNS Analyzer

For more information, see [IBM QRadar DNS Analyzer](#).

UBA : Potential Access to Blocklist Domain

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Potential Access to Blocklist Domain

Enabled by default

False

Default senseValue

5

Description

Detects events that indicate the user potentially accessed a blocklist domain. Requires the IBM QRadar DNS Analyzer app.

Required configuration

Before enabling this rule, you must install the IBM QRadar DNS Analyzer app. For more information, see [IBM QRadar DNS Analyzer](#).

Support rule

BB:UBA : DNS Common Filter

Log source types

IBM QRadar DNS Analyzer

UBA : Potential Access to DGA Domain

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Potential Access to DGA Domain

Enabled by default

False

Default senseValue

5

Description

Detects events that indicate the user potentially accessed a DGA (Domain Generated by Algorithm) domain. Requires the IBM QRadar DNS Analyzer app.

Required configuration

Before enabling this rule, you must install the IBM QRadar DNS Analyzer app. For more information, see [IBM QRadar DNS Analyzer](#).

Support rule

BB:UBA : DNS Common Filter

Log source types

IBM QRadar DNS Analyzer

UBA : Potential Access to Squatting Domain

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Potential Access to Squatting Domain

Enabled by default

False

Default senseValue

5

Description

Detects events that indicate the user potentially accessed a squatting domain. Requires the IBM QRadar DNS Analyzer app.

Required configuration

Before enabling this rule, you must install the IBM QRadar DNS Analyzer app. For more information, see [IBM QRadar DNS Analyzer](#).

Support rule

BB:UBA : DNS Common Filter

Log source types

IBM QRadar DNS Analyzer

UBA : Potential Access to Tunneling Domain

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Potential Access to Tunneling Domain

Enabled by default

False

Default senseValue

5

Description

Detects events that indicate the user potentially accessed a tunneling domain. Requires the IBM DNS Analyzer app.

Required configuration

Before enabling this rule, you must install the IBM QRadar DNS Analyzer app. For more information, see [IBM QRadar DNS Analyzer](#).

Support rule

BB:UBA : DNS Common Filter

Log source types

IBM QRadar DNS Analyzer

Threat intelligence

UBA : Detect IOCs For Locky

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Detect IOCs For Locky

Enabled by default

False

Default senseValue

10

Description

Detects user computers that show Indicators of Compromise (IOCs) for Locky by using URLs or IPs that are populated from X-Force campaign feeds.

Support rules

- BB:UBA : Common Log Source Filters
- BB:UBA : Detect Locky Using IP
- BB:UBA : Detect Locky Using URL

Required configuration

- Add the appropriate values to the following reference sets: UBA : IOCs-Locky IP and UBA : IOCs-Locky URL.
- Enable **Search assets for username, when username is not available for event or flow data** in **Admin Settings > UBA Settings**.

Log source types

All supported log sources.

UEBA : Detect IOCs for WannaCry

The QRadar User Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : Detect IOCs For WannaCry

Enabled by default

False

Default senseValue

10

Default senseValueSource

10

Description

Detects user computers that show Indicators of Compromise (IOCs) for WannaCry by using URLs, IPs, or hashes that are populated from X-Force campaign feeds.

Support rules

- BB:UBA : Common Log Source Filters
- BB:UBA : Detect WannaCry Using Hashes
- BB:UBA : Detect WannaCry Using IP
- BB:UBA : Detect WannaCry Using URL

Required configuration

- Add the appropriate values to the following reference sets: UBA : Malware Activity WannaCry - Hash, UBA : Malware Activity WannaCry - IP, and UBA : Malware Activity WannaCry - URL.
- Enable **Search assets for username, when username is not available for event or flow data** in **Admin Settings > UBA Settings**.

Log source types

All supported log sources.

UBA : Multiple Sessions to Monitored Log Sources (NIS Directive)

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : Multiple Sessions to Monitored Log Sources (NIS Directive)

Enabled by default

False

Default senseValue

15

Description

Detects more than 2 connections to the same QRadar log source system within 5 minutes from a single user.

Support rules

BB:UBA : Common Event Filters

BB:CategoryDefinition: Authentication Success

Required configuration

Add the appropriate values to the following reference sets: "UBA : Monitored Log Sources (NIS Directive)".

Log source types

Linux OS (EventID: CRYPTO_LOGIN, ANOM_ROOT_TRANS, Accepted Password, GRP_AUTH, session opened, Privilege escalation, CRED_ACQ, Accepted password, USER_LOGIN, Successful Login, password changed, LOGIN)

Microsoft Windows Security Event Log (EventID: Login succeeded for user, 18454, 193, 18455, 627, 4648, 1202, 680, 18453, 628, 621, 4624, 552, 672, 673_Attempt, 4672, 169, 10015, 10014, 678, 671, 6280, 4717, 4723, 4724, 540, 528, 673_Request, 673_Granted, 4776, 405, 5823, 1200, 682)

UBA : ShellBags Modified By Ransomware

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : ShellBags Modified By Ransomware

Enabled by default

False

Default senseValue

10

Description

Detects ShellBag registry modifications that indicate typical malware or ransomware behavior.

Support rules

BB:UBA : Common Event Filters

Log source types

Microsoft Windows Security Event Logs (EventID: 4657)

UEBA : User Accessing Risky IP Anonymization

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Accessing Risky IP Anonymization (previously called X-Force Risky IP, Anonymization)

Enabled by default

False

Default senseValueSource

10

Default senseValueDestination

10

Description

This rule detect when a local user or host is connecting to an external anonymization service.

Support rules

- X-Force Risky IP, Anonymization
- BB:UBA : Common Event Filters

Required configuration

- Set "Enable X-Force Threat Intelligence Feed" to Yes in **Admin Settings > System Settings**.
- Enable the following rule: X-Force Risky IP Anonymization.

Log source types

All supported log sources.

UBA : User Accessing Risky IP Botnet

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UBA : User Accessing Risky IP Botnet (previously called X-Force Risky IP, Botnet)

Enabled by default

False

Description

This rule detects when a local user or host is connecting to a botnet command and control server.

Support rules

- X-Force Risky IP, Botnet
- BB:UBA : Common Event Filters

Required configuration

- Set "Enable X-Force Threat Intelligence Feed" to Yes in **Admin Settings > System Settings**.
- Enable the following rule: X-Force Risky IP Botnet.

Log source types

All supported log sources.

UEBA : User Accessing Risky IP Dynamic

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Accessing Risky IP Dynamic (previously called X-Force Risky IP, Dynamic)

Enabled by default

False

Default senseValueSource

10

Description

This rule detects when a local user or host is connecting to a dynamically assigned IP address.

Support rules

- X-Force Risky IP, Dynamic
- BB:UBA : Common Event Filters

Required configuration

- Set "Enable X-Force Threat Intelligence Feed" to Yes in **Admin Settings > System Settings**.
- Enable the following rule: X-Force Risky IP Dynamic.

Log source types

All supported log sources.

UEBA : User Accessing Risky IP Malware

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Accessing Risky IP Malware (previously called X-Force Risky IP, Malware)

Enabled by default

False

Default senseValueSource

10

Description

This rule detects when a local user or host is connecting to a malware host.

Support rules

- X-Force Risky IP Malware
- BB:UBA : Common Event Filters

Required configuration

- Set "Enable X-Force Threat Intelligence Feed" to Yes in **Admin Settings > System Settings**.
- Enable the following rule: X-Force Risky IP Malware.

Log source types

All supported log sources.

UEBA : User Accessing Risky IP Spam

The QRadar User Entity Behavior Analytics (UEBA) app supports use cases based on rules for certain behavioral anomalies.

UEBA : User Accessing Risky IP, Spam (previously called X-Force Risky IP Spam)

Enabled by default

False

Default senseValueSource

10

Default senseValueDestination

10

Description

This rule detects when a local user or host is connecting to a spam-sending host.

Support rules

- X-Force Risky IP, Spam
- BB:UBA : Common Event Filters

Required configuration

- Set "Enable X-Force Threat Intelligence Feed" to Yes in **Admin Settings > System Settings**.
- Enable the following rule: X-Force Risky IP Spam.

Log source types

All supported log sources.

Supported QRadar content

Several rules were designed to feed events to QRadar User Entity Behavior Analytics (UEBA) from other apps. These rules require you to install the content for the other apps.

Content dependencies

For more information about other supported QRadar content and required apps, see the following table. The rules that are listed in the table are scored by the app.

Tip: To adjust the score, you must change it in the IBM QRadar Use Case Manager app or the Rules and Tuning page in the UEBA app.

Required Apps	Supported Rules
<u>IBM QRadar DNS Analyzer</u>	<u>“QRadar DNS Analyzer” on page 225</u>
<u>QRadar Network Insights Content for V7.3.0+</u>	<ul style="list-style-type: none"> • QNI : Confidential Content Being Transferred to Foreign Geography • QNI : Access to Improperly Secured Service - Certificate Expired • QNI : Access to Improperly Secured Service - Certificate Invalid • QNI : Potential Spam/Phishing Subject Detected from Multiple Sending Servers • QNI : Observed File Hash Seen Across Multiple Hosts • QNI : Observed File Hash Associated with Malware Threat • QNI : Potential Spam/Phishing Attempt Detected on Rejected Email Recipient • QNI : Access to Improperly Secured Service - Self Signed Certificate • QNI : Access to Improperly Secured Service - Weak Public Key Length
<u>IBM Security Reconnaissance Content</u>	<ul style="list-style-type: none"> • Local L2L TCP Scanner • Local L2L Windows Server Scanner • Local L2L Game Server Scanner • Local L2L DNS Scanner • Local L2L Mail Server Scanner • Local L2L Proxy Server Scanner • Local L2L IM Server Scanner • Local L2L Web Server Scanner • Local L2L P2P Server Scanner • Local L2L SNMP Scanner • Local L2L RPC Server Scanner • Local L2L UDP Scanner • Local L2L DHCP Scanner • Local L2L ICMP Scanner
<u>IBM QRadar Content for Sysmon</u>	<ul style="list-style-type: none"> • Detected a Possible Keylogger • Detected a New Unseen Process Started with a System User Privileges • Detected a Remotely Executed Process over Multiple Hosts • Process Started from Unusual Directories (Recycle.bin, ..) • A Hidden Network Share Has Been Added • Powershell Malicious Usage Detected • Powershell Malicious Usage Detected with Encoded Command

Required Apps	Supported Rules
	<ul style="list-style-type: none"> • Unusual Process (ex: word, iexplore, AcroRd..) • Launched a Command Shell • Command Shell Started With a System Privileges • Detected a Successful Login From a Compromised Host Into Other Hosts • Detected a Possible Credential Dumping Tool • Childless Process Launched/Spawned a Process • Process Launched From Temp Directory • Abnormal Parent for a System Process • Detected a Suspicious Svchost Process • A Network Share Has Been Accessed From a Compromised Host • An Administrative share Has Been Accessed • An Administrative share Has Been Accessed From a Compromised Machine • Process Launched From a Shared Folder and Created Thread into Another Process • Detected Excessive Usage of System Tools From a Single Machine • Excessive Failed Attempts to Access a Network Shared Resource From a Compromised Host • Excessive Failed Attempts to Access an Administrative Share From a Single source • Powershell Has Been Launched in a Compromised Host • PsExec Has Been Launched From a Compromised Host • Detected SMB Traffic From a Compromised Host Into Other Hosts • A Command Shell or Powershell Has been Launched From a Remote System • A Scheduled Task Has Been Created in a Compromised Host • A Malicious Service Has Been Installed in a System • Detected a Service Configured to Use Powershell • Detected a Service Configured to Use a Pipe
IBM QRadar Content Extension for Amazon AWS	<ul style="list-style-type: none"> • AWS Cloud: Cloud activity by root user • AWS Cloud: Critical EC2 Instance Has Been Stopped OR Terminated • AWS Cloud: Detected A Successful Login To AWS Console From Different Geographies • AWS Cloud: Logs Have Been Deleted / Disabled or Stopped

Required Apps	Supported Rules
	<ul style="list-style-type: none"> • AWS Cloud: Multiple Console Login Failures From Different Source IPs • AWS Cloud: Multiple Console Login Failures from Same Source IP • AWS Cloud: Multiple Failed API Requests From Different Source IPs • AWS Cloud: Multiple Failed API Requests From Same Source IP • AWS Cloud: Multiple Failed API Requests From The Same Username

Changed implementation for rules

The QRadar User Entity Behavior Analytics (UEBA) app no longer supports some rules. The functions that the rules provided are now integrated into the app, available in separate content packs, or implemented with machine learning models.

With UEBA 3.5.0 and later, during the upgrade, a one-time task runs to disable all unsupported UEBA rules found on the system. If any of the rules are enabled at a later time, they will not be disabled again by the application.

Although the following lists of UEBA rules and building blocks are no longer supported by the UEBA app, the rules or the functions that the rules provided are still available.

The following rules, and the functionality they provided, are now managed by Machine Learning:

- UBA : Abnormal Outbound Transfer Attempts
 - UBA : Abnormal Outbound Transfer Attempts Found
- UBA : Abnormal data volume to external domain
 - UBA : Abnormal data volume to external domain Found
- UBA : Abnormal visits to Risky Resources
 - UBA : Abnormal visits to Risky Resources Found
 - UBA : User Accessing Risky Resources
 - UBA : Risky Resources
- UBA : User Behavior, Session Anomaly by Destination
 - UBA : User Behavior, Session Anomaly by Destination Found
- UBA : User Event Frequency Anomaly - Categories
 - UBA : User Event Frequency Anomaly - Categories Found
- UBA : User Running New Process (replaced with *Process Usage* ML user model in UBA 3.8.0)
- UBA : User Volume Activity Anomaly - Traffic to External Domains
 - UBA : User Volume Activity Anomaly - Traffic to External Domains Found
- UBA : User Volume Activity Anomaly - Traffic to Internal Domains
 - UBA : User Volume Activity Anomaly - Traffic to Internal Domains Found
- UBA : User Volume of Activity Anomaly - Traffic
 - UBA : User Volume of Activity Anomaly - Traffic Found

The following rules and building blocks, and the functionality they provided, are now managed within the UEBA application:

- UBA : User Has Gone Dormant (no activity anomaly rule)

BB:UBA : Dormant User First Login (logic)
BB:UBA : Dormant User Subsequent Login (logic)
UBA : Username to User Accounts, Successful, Dormant

- New Account

UBA : Username to User Accounts, Successful, Observed
UBA : Username to User Accounts, Successful, Recent
UBA : Username to User Accounts, Successful, Recent Update
BB:UBA : User First Time Access (logic)

The following rules and building blocks, and the functionality they provided, are now handled by allowing non-UEBA rules to work with UEBA:

- QNI

UBA : QNI - Access to Improperly Secured Service - Certificate Expired
UBA : QNI - Access to Improperly Secured Service - Certificate Invalid
UBA : QNI - Access to Improperly Secured Service - Self Signed Certificate
UBA : QNI - Access to Improperly Secured Service - Weak Public Key Length
UBA : QNI - Observed File Hash Associated with Malware Threat
UBA : QNI - Observed File Hash Seen Across Multiple Hosts
UBA : QNI - Potential Spam/Phishing Attempt Detected on Rejected Email Recipient
UBA : QNI - Potential Spam/Phishing Subject Detected from Multiple Sending Servers
UBA : QNI - Confidential Content Being Transferred to Foreign Geography

- SYSMON

UBA : Suspicious PowerShell Activity
UBA : Suspicious PowerShell Activity (Asset)
UBA : Suspicious Command Prompt Activity
UBA : User Access Control Bypass Detected (Asset)
UBA : Suspicious Scheduled Task Activities
UBA : Suspicious Service Activities
UBA : Suspicious Service Activities (Asset)
UBA : Suspicious Entries in System Registry (Asset)
UBA : Suspicious Image Load Detected (Asset)
UBA : Suspicious Pipe Activities (Asset)
UBA : Suspicious Activities on Compromised Hosts
UBA : Suspicious Activities on Compromised Hosts (Asset)
UBA : Suspicious Administrative Activities Detected
UBA : Process Creating Suspicious Remote Threads Detected (Asset)
UBA : Common Exploit Tools Detected
UBA : Common Exploit Tools Detected (Asset)
UBA : Malicious Process Detected
UBA : Network Share Accessed

- Recon

UBA : Unusual Scanning of DHCP Servers Detected
UBA : Unusual Scanning of DNS Servers Detected
UBA : Unusual Scanning of Database Servers Detected
UBA : Unusual Scanning of FTP Servers Detected
UBA : Unusual Scanning of Game Servers Detected
UBA : Unusual Scanning of Generic ICMP Detected
UBA : Unusual Scanning of Generic TCP Detected
UBA : Unusual Scanning of Generic UDP Detected
UBA : Unusual Scanning of IRC Servers Detected

UBA : Unusual Scanning of LDAP Servers Detected
UBA : Unusual Scanning of Mail Servers Detected
UBA : Unusual Scanning of Messaging Servers Detected
UBA : Unusual Scanning of P2P Servers Detected
UBA : Unusual Scanning of Proxy Servers Detected
UBA : Unusual Scanning of RPC Servers Detected
UBA : Unusual Scanning of SNMP Servers Detected
UBA : Unusual Scanning of SSH Servers Detected
UBA : Unusual Scanning of Web Servers Detected
UBA : Unusual Scanning of Windows Servers Detected

Chapter 9. Machine Learning Analytics app

The Machine Learning Analytics (ML) app extends the capabilities of your QRadar system and the QRadar User Entity Behavior Analytics (UEBA) app by adding use cases for machine learning analytics. With the machine learning analytics models, you can gain additional insight into user behavior with predictive modeling. The ML app helps your system to learn the expected behavior of the users in your network.



Attention: You must have admin permissions to install the ML app.

Note: For the best experience with Machine Learning, you should consider running the UEBA app and the ML app on an App Host. For more information, see [App Host](#).

You should set up the machine learning container to be as large as possible. After you install the ML app, you cannot increase or decrease the container size.

Important:

- It is best to enable Machine Learning Analytics Settings one day after you initially configure the UEBA app. This waiting period ensures that the UEBA app has sufficient time to create risk profiles for users.
- The QRadar Console limits the amount of memory that can be used by apps. The ML app installation size options are based on how much memory QRadar currently has for applications.
 - The minimum amount of free memory required to install the ML app is 2 GB. However, 5 GB or higher is recommended.
 - The number of users monitored by the ML app depends on the ML app installation size and the specific Machine Learning analytic. Starting at 5 GB, the maximum number of monitored users by non peer group Machine Learning model is 40,000 per 5 GB up to 220,000 users total. For example, 5 GB would be up to 40,000 users, 15 GB would be up to 120,000 users, and 40 GB would be up to 220,000 users for non peer group models. And Starting at 5 GB, the maximum number of monitored users by peers group Machine Learning model is 2500 per 5 GB up to 12,500 users total for peers group model. For example, 5 GB would be up to 2500 users, 20 GB would be up to 10,000 users, and 25 GB would be up to 12500 users for peers group models.
- The installation might fail due to a lack of available memory. This situation can occur if the amount of memory available for applications is decreased because other applications are installed.

Known issues for Machine Learning Analytics

The Machine Learning Analytics (ML) app has required information for installation and known issues.

The Machine Learning Analytics app has the following known issues:

- The Machine Learning Analytics app might show warning messages in the Status of Machine Learning section. For more information, see [“Machine Learning app status shows warning on dashboard”](#) on page 274.
- The installation might fail due to a lack of available memory. This situation can occur on 128 GB consoles if several other apps are already installed and less than 10 GB remains for the ML app to use. If the installation fails, the error message "FAILED" is displayed. To remedy this situation, uninstall some of the other apps and then try again.

Prerequisites for installing the Machine Learning Analytics app

Before you install the Machine Learning Analytics app, ensure that you meet the requirements.

You must meet the following system requirements and fully install and configure the User Entity Behavior Analytics (UEBA) app before you can install the Machine Learning Analytics app.

Component	Minimum requirements
System memory	2 GB of free memory from the QRadar application pool of memory
IBM QRadar version	Verify that you have IBM Security QRadar 7.4.3 Fix Pack 6 or later installed.
Sense DSM	Install the DSM RPM file.
UBA app	<ul style="list-style-type: none"> • Install UBA. • Configure the UEBA Settings. • Click the User Entity Analytics tab and confirm that the UEBA dashboard contains user data.

Installing the IBM Sense DSM manually

The UEBA app and the Machine Learning Analytics app use the following IBM Sense DSM files to add user risk scores and offenses into QRadar.

- For QRadar 7.4.0 and later: DSM-IBMSense-7.4-20200812144513.noarch.rpm

Restriction: Uninstalling a Device Support Module (DSM) is not supported in QRadar.

1. Copy the DSM RPM file to your QRadar Console.
2. Use SSH to log in to the QRadar host as the root user.
3. Go to the directory that includes the downloaded file.
4. Type the following command:

```
rpm -Uvh <rpm_filename>
```

5. From the **Admin** settings, click **Advanced** > **Deploy Full Configuration**.

Note: For instructions on installing and configuring the UEBA app, see [QRadar User Behavior Analytics](#).

Related tasks

[“Installing the User Entity Behavior Analytics app” on page 25](#)

Use the IBM QRadar Extension Management tool to upload and install your app archive directly to your QRadar Console.

[“Configuring UEBA settings” on page 31](#)

To view information in the IBM QRadar User Entity Behavior Analytics (UEBA) app, you must configure UEBA application settings.

Installing the Machine Learning Analytics app

As a QRadar Admin, you can install the Machine Learning Analytics (ML) app after you have installed the QRadar User Entity Behavior Analytics (UEBA) app from the Extension Manager.

Before you begin

Make sure you have completed all of the [Prerequisites for installing the Machine Learning Analytics app](#).

For the best experience with Machine Learning, you should consider running the UEBA app and the ML app on an App Host. For more information, see [App Host](#).

About this task

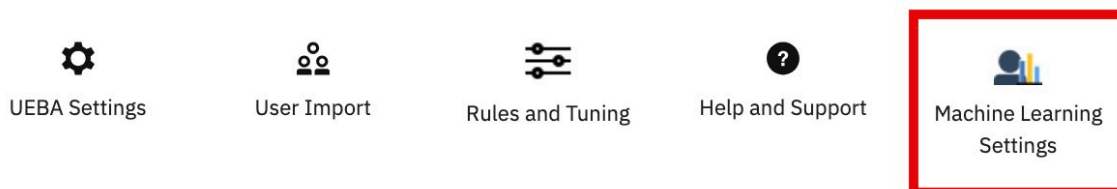
After you install the User Entity Behavior Analytics (UEBA) app, you can install the ML app from the Machine Learning Settings page.

You must have admin permissions to view Machine Learning Settings.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. Click the **Machine Learning Settings** icon.
 - Click **Apps > User Entity Analytics > Machine Learning Settings**.

User Entity Analytics



3. On the **Machine Learning Settings** page, click **Install ML App**.
4. At the prompt, click **Yes** to install the app. The ML app takes several minutes to install.

What to do next

When the installation is complete, you can enable Machine Learning use cases and then click **Save Configuration**.

UEBA dashboard with Machine Learning


The IBM QRadar User Entity Behavior Analytics (UEBA) app with Machine Learning Analytics includes the Machine Learning model status and additional details for the selected user.

Dashboard

After you enable the Machine Learning models, click the **User Entity Analytics** tab to open the main UEBA Overview (Dashboard) page.

The Status of Machine Learning Models section shows you the ingestion and the building progress for each model you have enabled.


- The purple progress bar indicates that the model is ingesting data.
- The blue progress bar indicates that the model is building.
- The green progress bar indicates that the model is training. Note: If the model is not receiving data, then it remains in training until enough data is received.
- The green check mark indicates that the model is enabled.
- The yellow warning icon indicates a problem was encountered during the model building phase. See [“Machine Learning app status shows warning on dashboard” on page 274](#).

Click the **ML Settings** icon  to open the Machine Learning Analytics page and edit the configuration for the machine learning models.

Note: If you edit the configuration after it has been saved, a new model will be built and the time to wait for the ingestion and model building is reset.

The following image shows an example of a Machine Learning models status widget in the UEBA 4.0.0 light theme UI.

Status of machine learning models

Access activity		
Data downloaded		
Defined peer group		
Learned peer group		

User details page

You can click a user name from anywhere in the app to see details for the selected user.

You can learn more about the user's activities with the *event viewer* pane. The event viewer pane shows information about a selected activity or point in time. Clicking an event in the event viewer pane reveals more details such as syslog events and payload information. The event viewer pane is available for all donut and line graphs on the **User details** page.

The following tables describes the Machine Learning Analytics graphs available on the **User Details** page.

Table 6. Names and descriptions of time series ML graphs

Time series graphs	Description
<ul style="list-style-type: none"> • Access activity • Aggregated activity • Authentication activity • Data uploaded to remote networks • Data downloaded • DML events • DDL events • Large HTTP transfers • Outbound transfer attempts • Risk posture • Suspicious activity • Successful access and authentication activity 	<p>Note: All custom models use this graph type.</p> <p>Shows actual and expected user activity behavior patterns. The actual values are the number of events for that user during the selected time period. The expected values are the predicted number of events for that user during the selected time period. A red circle indicates that an anomaly was detected and a sense event was generated by machine learning.</p> <p>On the times series graph, you can:</p> <ul style="list-style-type: none"> • Click a node and get a query listing of the events. • Click the Calendar icon to specify a time and date. <p>The following image shows an example of a time series graph in the UEBA 4.0.0 light theme UI.</p> <div style="border: 1px solid #ccc; padding: 10px;"> <p>Risk posture Nov 30 - Dec 2 </p> </div>

Table 7. Name and description of ML distribution graph

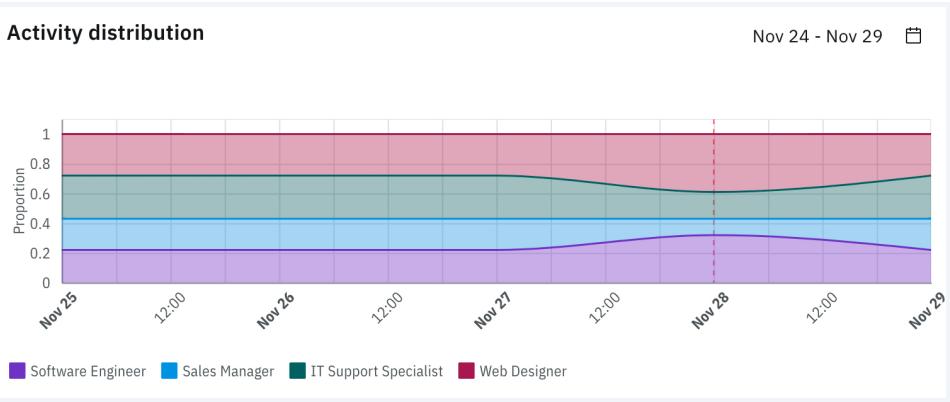
Distribution graph	Description
Activity distribution	<p>Shows dynamic behavior clusters for all users that are monitored by machine learning. The clusters are inferred by the activity categories for all users that are monitored by machine learning. The actual values are the percent match to that cluster. The expected values are the predicted percent match to that cluster. Each color in the graph represents a unique dynamic behavior cluster for all users monitored by machine learning. A color used to denote a particular group is the same for all users. A red vertical line indicates that an anomaly was detected and a sense event was generated by machine learning.</p> <p>On the graph, you can:</p> <ul style="list-style-type: none"> • Hover over each cluster to view the actual and predicted activity percentiles and the top 3 contributing categories. • Click the Calendar icon to specify a date range. <p>The following image shows an example of an activity distribution graph in the UEBA 4.0.0 light theme UI.</p>  <p>Activity distribution Nov 24 - Nov 29 📅</p> <p>Proportion</p> <p>1 0.8 0.6 0.4 0.2 0</p> <p>Nov 25 12:00 Nov 26 12:00 Nov 27 12:00 Nov 28 12:00 Nov 29</p> <p> ■ Software Engineer ■ Sales Manager ■ IT Support Specialist ■ Web Designer </p>

Table 8. Names and descriptions of peer group ML graphs

Peer group graphs	Description																		
<ul style="list-style-type: none"> • Defined peer group • Learned peer group 	<p>Shows how much a user's event activity deviates from that of their peer group. A red circle indicates that an anomaly was detected and a sense event was generated by machine learning. Defined group is the LDAP group chosen in the model settings. Behavior detected as are the groups the user behavior was similar to during the day. Deviation from peer group signifies the percentage a user has deviated from their defined peer group. Confidence is based on the amount of data gathered to build the model from users in the group to make accurate predictions. An alert is triggered if the deviation and the confidence both exceed their thresholds.</p> <p>To view the peer group analytic, you must configure user imports to gather user grouping properties to meet minimum requirements. Select the grouping property on the configuration page that represents the groups to be modeled. See “Tuning user import configurations” on page 41 for details on configuring the custom group.</p> <p>On the graph, you can:</p> <ul style="list-style-type: none"> • Click a data point to view the Peers in "your peer group" table. • Click the Calendar icon to specify a date range. <p>The Peers in "your peer group" table shows you the riskiest users in the current user's group. You can:</p> <ul style="list-style-type: none"> • Click a user name to open the User Details page • Click the drop-down list to select the user attributes to display • Search to filter the user names <p>The following image shows an example of a defined peer group graph with custom groupings in the UEBA 4.0.0 light theme UI.</p> <div data-bbox="527 1150 1453 1522"> <p>Defined peer group: Custom group Nov 27 - Dec 2 </p> <div data-bbox="1031 1155 1282 1333" style="border: 1px solid gray; padding: 5px;"> <p>Anomaly detected</p> <p>Nov 29, 7:00 PM</p> <p>Defined group: custom_group_D</p> <p>Behavior detected as: custom_group_B</p> <p>Deviation from peer group: 96%</p> <p>Confidence: 100%</p> </div> </div> <div data-bbox="527 1543 1453 1921"> <p>Peers in "custom_group_D" December 1, 2020 7:00 PM</p> <p>🔍</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Risk score</th> <th>Job title</th> </tr> </thead> <tbody> <tr> <td>group_D-10_ariel_D_...</td> <td>71</td> <td>Web Designer</td> </tr> <tr> <td>group_D-11_ariel_D_...</td> <td>84</td> <td>Sales Manager</td> </tr> <tr> <td>group_D-12_ariel_D_...</td> <td>64</td> <td>Sales Manager</td> </tr> <tr> <td>group_D-13_ariel_D_...</td> <td>99</td> <td>Web Designer</td> </tr> <tr> <td>group_D-14_ariel_D_...</td> <td>85</td> <td>Sales Manager</td> </tr> </tbody> </table> </div>	Name	Risk score	Job title	group_D-10_ariel_D_...	71	Web Designer	group_D-11_ariel_D_...	84	Sales Manager	group_D-12_ariel_D_...	64	Sales Manager	group_D-13_ariel_D_...	99	Web Designer	group_D-14_ariel_D_...	85	Sales Manager
Name	Risk score	Job title																	
group_D-10_ariel_D_...	71	Web Designer																	
group_D-11_ariel_D_...	84	Sales Manager																	
group_D-12_ariel_D_...	64	Sales Manager																	
group_D-13_ariel_D_...	99	Web Designer																	
group_D-14_ariel_D_...	85	Sales Manager																	

The following Machine Learning user models are not represented by a graph:

- Lateral Movement: Internal Destination Port Activity
- Lateral Movement: Network Zone Access
- Lateral Movement: Internal Asset Usage
- Process Usage

Related tasks

“Machine Learning user models” on page 247

To view information in the Machine Learning Analytics app, you must configure Machine Learning settings for User Models.

Uninstalling the Machine Learning Analytics app

Uninstall the Machine Learning Analytics app from the Machine Learning Settings page.

About this task

Before you uninstall the UEBA app, you must complete the following procedure for uninstalling the ML app. If you do not uninstall the ML app before you uninstall UEBA, you must remove it from the interactive API documentation interface.


Procedure


1. On the navigation menu (☰), click **Admin**.
2. Click **Apps > User Entity Analytics > Machine Learning Settings**.

User Entity Analytics


UEBA Settings


User Import


Rules and Tuning


Help and Support



3. On the Machine Learning Settings screen, click **Uninstall ML App**.
4. At the uninstall prompt, click **Yes**.

What to do next

You must clear your browser cache before logging back in to the QRadar Console.

Chapter 10. Machine Learning user models

To view information in the Machine Learning Analytics app, you must configure Machine Learning settings for User Models.

About this task

You can see the type of model and the number of users in each model. You can also view the list of users in the model by clicking on the count.

On the User Models page, you can take the following actions:

- Enable up to 17 models
- Select a model to edit the default settings.
- Create your own custom models with the included templates.



Attention: After you configure or modify your settings, it takes a minimum of 1 hour to ingest data, build an initial model, and see initial results for users. For more information, see [“Machine learning analytic requirements”](#) on page 270.

Active users are monitored continuously. If a user has no activity for 28 days, the user and the user's data are removed from the model. If the user is active again, they will return as a new user.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. Click **Apps > User Entity Analytics > Machine Learning Settings**.
3. On the **Machine Learning Settings** page, click **Enabled** to turn on the selected model.
4. Click the model name if you want to edit the default settings.
5. In the **Risk value of sense event** field, enter the amount to increase the user's risk score when a sense event is triggered. The default value is 5.
6. Enable the toggle to scale the risk value. When enabled, the base risk value is multiplied by a factor (range 1 - 10). This factor is determined by how much the user deviates from their expected behavior and not just that they deviated.
7. In the **Confidence interval to trigger anomaly** field, enter the percentage for how confident the machine learning algorithm should be before it triggers an anomalous event. The default value is 0.95.
8. In the **Data Retention Period** field, set the number of days you want to save the model data. The default value is 30.
9. The **Show graph on User Details page** toggle is enabled by default to display the selected graph on the **User Details** page. If you do not want to display a graph on the **User Details** page, click the toggle.
10. For Peer Group and Activity Distribution models, in the **Group By** field, select the group that you want the selected peer group analytic to use.
11. In the **AQL Search Filter** field, you can add an AQL filter to narrow the data that the analytic queries for in QRadar. By filtering with an AQL query, you can reduce the number of users or the types of data the analytic is analyzing. Before you save your settings, click **Validate Query** to launch a full AQL query in QRadar so that you can review the query and verify the results.

Important: If you modify the AQL filter, the existing model is marked invalid and is then rebuilt. The length of time the rebuild takes depends on the amount of data that is returned by the modified filter.

You can filter on specific log sources, network names, or reference sets that contain specific users. See the following examples:

- **REFERENCESETCONTAINS('Important People', username)**
- **LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')**
- **INCIDR('172.16.0.0/12', sourceip) or INCIDR('10.0.0.0/8', sourceip) or INCIDR('192.168.0.0/16', sourceip)**

For more information, see [Ariel Query Language](#).

12. Click **Save**.

Results

It can take a minimum of 1 hour for the app to ingest data and build an initial model.

Individual (Numeric) user models

Individual (Numeric) user models calculate a specific numeric value for the user for the past 10 days. When the user deviates outside of the predicted range, the Machine Learning model determines with a high level of confidence that the event is anomalous.

Related concepts

[Individual \(Observable\) user models](#)

[Individual \(Observable\) user models](#) calculate a set of attributes and their corresponding event count for the user for the past 10 days. When the user deviates outside the predicted range or uses a new value, the ML model determines with a high level of confidence that the event is anomalous.

[Peer group models](#)

[Peer group models](#) calculate a set of attributes with their corresponding event count numeric value for the user for the past 30 days. The ML model determines with a high level of confidence that the user deviated outside of the group.

[Machine learning analytic requirements](#)

[Machine learning models](#) can take some time to train and build based on different analytic requirements.

Related tasks

[Creating a custom model](#)

[Creating a custom model](#) Create a custom model to measure and baseline a numeric feature for a person per hour.

[Peer group model grouping requirements](#)

[Peer group model grouping requirements](#) Peer group machine learning models require grouping properties to meet minimum requirements.

Access activity

The *Access Activity* model tracks a user's activity in the Access high-level category and creates a learned behavioral model for each hour of the day.

Enable the *Access Activity* machine learning model to display the user's activity in the Access high-level category on the **User Details** page. If the user's Access activity deviates from the learned behavior, it is deemed suspicious and a Sense Event is generated to increase the user's risk score.

Event name

UBA : Abnormal increase in Access activity

sensevalue

5

Required configuration

System is monitoring events that have QRadar high-level category of Access.

Log source types

Akamai KONA, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arbor Networks Pravail, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, BeyondTrust PowerBroker, Bit9 Security Platform, Blue Coat Web Security Service, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, Carbon Black Protection, Centrify Identity Platform, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Cloud Web Security, Cisco FireSIGHT Management Center, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Firewall Filter, CorreLog Agent for IBM zOS, Custom Rule Engine, DCN DCS/DCRS Series, EMC VMWare, Epic SIEM, Event CRE Injected, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix K/N/S Series Switch, Extreme NAC, Extreme Stackable and Standalone Switches, Extreme XSR Security Routers, F5 Networks BIG-IP AFM, F5 Networks BIG-IP ASM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Fidelis XPS, Flow Classification Engine, Forcepoint Sidewinder, Forcepoint V Series, Fortinet FortiGate Security Gateway, Foundry Fastiron, H3C Comware Platform, HP Network Automation, HP ProCurve, HP Tandem, Honeycomb Lexicon File Integrity Monitor, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Server, IBM Bluemix Platform, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM Guardium, IBM IMS, IBM Informix® Audit, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Manager, IBM Security Network IPS (GX), IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Illumio Adaptive Security Platform, Imperva Incapsula, Imperva SecureSphere, Infoblox NIOS, Itron Smart Meter, Juniper DX Application Acceleration Platform, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper WirelessLAN, Juniper vGW, Kaspersky Security Center, Kisco Information Systems SafeNet/i, Lieberman Random Password Manager, Linux OS, Linux iptables Firewall, Mac OS X, McAfee Application/Change Control, McAfee Network Security Platform, McAfee ePolicy Orchestrator, Microsoft Azure, Microsoft Exchange Server, Microsoft Hyper-V, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, NGINX HTTP Server, Netskope Active, Nortel Contivity VPN Switch, Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, Okta, Open LDAP Software, OpenBSD OS, Oracle Audit Vault, Oracle BEA WebLogic, Oracle RDBMS OS Audit Record, Palo Alto PA Series, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, Salesforce Security Auditing, Snort Open Source IDS, Solaris Operating System Authentication Messages, Solaris Operating System DHCP Logs, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Sophos Enterprise Console, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sun ONE LDAP, Sybase ASE, Symantec Critical System Protection, Symantec Encryption Management Server, Symantec Endpoint Protection, Symantec Gateway Security (SGS) Appliance, Symantec System Center, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend InterScan VirusWall, Trend Micro Deep Security, Universal DSM, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, Zscaler Nss, genua genugate, iT-CUBE agileSI

Aggregated Activity

The *Aggregated Activity* model tracks a user's general activity by time and creates a model for the predicted weekly behavior patterns.

Enable the *Aggregated Activity* machine learning model to display the user's general activity by time on the **User Details** page. If the user's activity deviates from the learned behavior, it is deemed suspicious and a Sense Event is generated to increase the user's risk score.

Event name

UBA : Abnormal increase in User activity

sensevalue

5

Log source types

Any log source with events that provide a username.

Authentication Activity

The *Authentication Activity* model tracks a user's activity in the Authentication high-level category and creates a learned behavioral model for each hour of day.

Enable the *Authentication Activity* machine learning model to display the user's activity in the Authentication high-level category on the **User Details** page. If the user's Authentication activity deviates from the learned behavior, it is deemed suspicious and a Sense Event is generated to increase the user's risk score.

Event name

UBA : Abnormal increase in Authentication activity

sensevalue

5

Required configuration

System is monitoring events that have QRadar high-level category of Authentication.

Log source types

3Com 8800 Series Switch, APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arbor Networks Pravail, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Introspect, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCARD CRYPTOSHIELD, Carbon Black Protection, Centrify Identity Platform, Centrify Infrastructure Services, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco FireSIGHT Management Center, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Cloudera Navigator, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, CyberGuard TSP

Firewall/VPN, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, ESET Remote Administrator, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Matrix K/N/S Series Switch, Extreme NAC, Extreme NetsightASM, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, Extreme XSR Security Routers, F5 Networks BIG-IP APM, F5 Networks BIG-IP ASM, F5 Networks BIG-IP LTM, F5 Networks FirePass, FireEye, Flow Classification Engine, Forcepoint Sidewinder, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP ProCurve, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM Bluemix Platform, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM Guardium, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Directory Server, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Illumio Adaptive Security Platform, Imperva SecureSphere, Infoblox NIOS, Itron Smart Meter, Juniper Junos OS Platform, Juniper Junos WebApp Secure, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, LightCyber Magna, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Network Security Platform, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft Azure, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft Hyper-V, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft SharePoint, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDoS Secure, Netskope Active, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, Open LDAP Software, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, PostFix MailTransferAgent, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Encryption Management Server, Symantec Endpoint Protection, ThreatGRID Malware Threat Intelligence Platform, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Discovery Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, VMware vShield, Vectra Networks Vectra, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

Data Downloaded

The *Data Downloaded* model monitors data that is downloaded for each user and then alerts on abnormal behavior.

Enable the *Data Downloaded* machine learning model to display data that is downloaded for each user on the **User Details** page. When the actual volume of data that is downloaded exceeds the model's predicted number, a Sense Event is generated to increase the user's risk score.

Event name

UBA : Abnormal Data Downloaded

sensevalue

5

Required configuration

Custom event property "Bytes Received" must exist for the desired log source type.

Log source types

Pulse Secure Pulse Connect Secure, Fortinet FortiGate Security Gateway, Blue Coat SG Appliance, Juniper SRX Series Services Gateway, Microsoft ISA, Citrix NetScaler

Data Uploaded to Remote Networks

The *Data Uploaded to Remote Networks* model monitors external domain data usage for each user and alerts on abnormal behavior.

Enable the *Data Uploaded to Remote Networks* machine learning model to display the actual and expected (learned) amount of local to remote upload volume for each user on the **User Details** page. When the actual number of external domain data usage exceeds the model's predicted number, a Sense Event is generated to increase the user's risk score.

Event name

UBA : Abnormal Volume of Data to External Domains

sensevalue

5

Required configuration

Custom event property "Bytes Sent" must exist for the desired log source type.

Log source types

Pulse Secure Pulse Connect Secure, Fortinet FortiGate Security Gateway, Blue Coat SG Appliance, Juniper SRX Series Services Gateway, Microsoft ISA, Citrix NetScaler

DDL events

The DDL (Data Definition Language) Events model tracks a user's DDL events in time and creates a model for the predicted weekly score.

Enable the DDL (Data Definition Language) Events model to track a user's DDL events in time and create a model for the predicted weekly score. If the user's score deviates from the learned one, it is deemed as suspicious behavior and a Sense Event is generated to increase the user's risk score.

Event name

UBA : Increase in DDL events

sensevalue

5

Log source types

Application Security DbProtect, IBM DB2, IBM Guardium, Imperva SecureSphere, Microsoft SQL Server, Oracle Audit Vault, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record

DML events

The DML (Data Manipulation Language) events model tracks a user's DML events in time and creates a model for the predicted weekly score.

Enable the DML events model to track a user's DML events in time and create a model for the predicted weekly score. If the user's score deviates from the learned one, it is deemed suspicious behavior and a Sense Event is generated to increase the user's risk score.

Event name

UBA : Increase in DML events

sensevalue

5

Log source types

Application Security DbProtect, IBM DB2, IBM Guardium, Imperva SecureSphere, Microsoft SQL Server, Oracle Audit Vault, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record

HTTP Data Transfer Activity

The *HTTP Data Transfer Activity* model tracks a user's HTTP data transfer events in time and creates a model for the predicted weekly score.

Enable the *HTTP Data Transfer Activity* model to track a user's HTTP data transfer events in time and create a model for the predicted weekly score. If the user's score deviates from the learned one, it is deemed suspicious behavior and a Sense Event is generated to increase the user's risk score.

Event name

UBA : Large HTTP transfers

sensevalue

5

Required configuration

You must define the following properties:

- *Bytes Sent*
- *URL*

Log source types

Log sources that contain events with both properties defined and that use destination port 80 or 443.

Outbound Transfer Attempts

The *Outbound Transfer Attempts* machine learning model monitors outbound traffic usage for each user and alerts on abnormal behavior.

Enable the *Outbound Transfer Attempts* model to display outbound traffic usage for each user on the **User Details** page. When the actual number of transfer attempts exceeds the model's predicted number, a Sense Event is generated to increase the user's risk score.

Event name

UBA : Abnormal Outbound Transfer Attempts

sensevalue

5

Required configuration

Custom event property *Bytes Sent* must exist for the desired log source type.

Log source types

Pulse Secure Pulse Connect Secure, Fortinet FortiGate Security Gateway, Blue Coat SG Appliance, Juniper SRX Series Services Gateway, Microsoft ISA, Citrix NetScaler

Risk Posture

The *Risk Posture* model tracks a user's risky activity by the rate of sense events generated and creates a baseline model.

Enable the *Risk Posture* model to display the user's risk score deviation on the **User Details** page. If the user's risky activity deviates from the baseline, it is deemed suspicious and a sense event is generated to increase the user's overall risk score.

Event name

UBA : Deviation from normal Risk posture

sensevalue

5

Required configuration

UBA is configured and sense events are being created.

Log source types

Any log sources with events that trigger sense events.

Successful Access and Authentication Activity

The *Successful Access and Authentication Activity* model tracks a user's successful authentication and access events by time and creates a model for the predicted weekly behavior patterns.

Enable the *Successful Access and Authentication Activity* model to track a user's successful authentication and access events by time and create a model for the predicted weekly behavior patterns. If the user's activity deviates from the learned behavior, it is deemed suspicious and a Sense Event is generated to increase the user's risk score.

Event name

UBA : Increase in successful access and authentication

sensevalue

5

Required configuration

You must define the following properties:

- *Bytes Sent*
- *URL*

Log source types

Log sources associated to the high-level category Access and high-level category Authentication.

Suspicious Activity

The *Suspicious Activity* model tracks a user's activity in the Suspicious Activity high-level category and creates a learned behavioral model for each hour of the day.

Enable the *Suspicious Activity* machine learning model to display the actual and expected (learned) amount of Suspicious Activity high-level category on the **User Details** page. If the user's Suspicious Activity deviates from the learned behavior, it is deemed suspicious and a Sense Event is generated to increase the user's risk score.

Event name

UBA : Abnormal increase in Suspicious activity

sensevalue

5

Required configuration

System is monitoring events that have QRadar high level category of Suspicious Activity.

Log source types

Log source types: 3Com 8800 Series Switch, Akamai KONA, Application Security DbProtect, Arbor Networks Peakflow SP, Aruba Introspect, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CRE System, Carbon Black, Carbon Black Protection, Check Point, Cilasoft QJRN/400, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco Meraki, Cisco NAC Appliance, Cisco PIX Firewall, Cisco Stealthwatch, Cisco Umbrella, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), CloudLock Cloud Security Fabric, CrowdStrike Falcon Host, Custom Rule Engine, CyberArk Privileged Threat Analytics, CyberGuard TSP Firewall/VPN, Damballa Failsafe, EMC VMWare, ESET Remote Administrator, Enterprise-IT-Security.com SF-Sherlock, Event CRE Injected, Exabeam, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiGuard, Extreme HiPath, Extreme Matrix K/N/S Series Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme XSR Security Routers, F5 Networks BIG-IP AFM, F5 Networks BIG-IP ASM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Fair Warning, Fidelis XPS, FireEye, Flow Classification Engine, Forcepoint Sidewinder, ForeScout CounterACT, Fortinet FortiGate Security Gateway, FreeRADIUS, H3C Comware Platform, Huawei AR

Series Router, Huawei S Series Switch, IBM AIX Server, IBM BigFix Detect, IBM Guardium, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM Resource Access Control Facility (RACF), IBM Security Network IPS (GX), IBM Security Trusteer Apex Advanced Malware Protection, IBM WebSphere Application Server, IBM i, IBM z/OS, ISC BIND, Imperva SecureSphere, Juniper Junos OS Platform, Juniper Junos WebApp Secure, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper WirelessLAN, Kaspersky CyberTrace, Kaspersky Security Center, Kisco Information Systems SafeNet/i, Lastline Enterprise, LightCyber Magna, Linux DHCP Server, Linux OS, McAfee Application/Change Control, McAfee Network Security Platform, McAfee ePolicy Orchestrator, Microsoft DHCP Server, Microsoft DNS Debug, Microsoft Endpoint Protection, Microsoft Hyper-V, Microsoft Operations Manager, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niksun 2005 v3.5, Nortel Contivity VPN Switch, Nortel Secure Router, Nortel VPN Gateway, OS Services Qidmap, OSSEC, ObserveIT, Onapsis Inc Onapsis Security Platform, Palo Alto Endpoint Security Manager, Palo Alto PA Series, PostFix MailTransferAgent, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler, SAP Enterprise Threat Detection, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Samhain HIDS, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, SolarWinds Orion, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Sophos Enterprise Console, Sophos PureMessage, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Symantec Endpoint Protection, Symantec System Center, ThreatGRID Malware Threat Intelligence Platform, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Discovery Inspector, Trend Micro Deep Security, Universal DSM, Vectra Networks Vectra, Verdasys Digital Guardian, WatchGuard Fireware OS, Zscaler Nss, genua genugate, iT-CUBE agileSI

Individual (Observable) user models

Individual (Observable) user models calculate a set of attributes and their corresponding event count for the user for the past 10 days. When the user deviates outside the predicted range or uses a new value, the ML model determines with a high level of confidence that the event is anomalous.

Related concepts

Individual (Numeric) user models

Individual (Numeric) user models calculate a specific numeric value for the user for the past 10 days. When the user deviates outside of the predicted range, the Machine Learning model determines with a high level of confidence that the event is anomalous.

Peer group models

Peer group models calculate a set of attributes with their corresponding event count numeric value for the user for the past 30 days. The ML model determines with a high level of confidence that the user deviated outside of the group.

Machine learning analytic requirements

Machine learning models can take some time to train and build based on different analytic requirements.

Related tasks

Creating a custom model

Create a custom model to measure and baseline a numeric feature for a person per hour.

Peer group model grouping requirements

Peer group machine learning models require grouping properties to meet minimum requirements.

Lateral Movement : Internal Asset Usage

The *Lateral Movement : Internal Asset Usage* model tracks a user's internal destination asset activity by time and creates a model for the predicted weekly behavior patterns.

Enable the *Lateral Movement : Internal Asset Usage* model to track a user's internal destination asset activity by time and create a model for the predicted weekly behavior patterns. If the user's activity

deviates from the learned behavior, it is deemed suspicious and a Sense Event is generated to increase the user's risk score. An event to increase the score is also sent when a new internal asset (destination IP) is used by the user.

Event name (new activity)

UBA : New internal asset used

Event Name (activity deviation)

UBA : Abnormal usage of internal asset

sensevalue

5

Required configuration

Configuring the Network Hierarchy will help with the accuracy of determining internal destination addresses.

Log source types

All events that have a defined username and local destination IP.

Lateral Movement : Internal Destination Port Activity

The *Lateral Movement : Internal Destination Port Activity* model tracks a user's activity to internal destination port activity by time and creates a model for the predicted weekly behavior patterns.

Enable the *Lateral Movement : Internal Destination Port Activity* model to track a user's activity to internal destination port activity by time and create a model for the predicted weekly behavior patterns. If the user's activity deviates from the learned behavior, it is deemed suspicious and a Sense Event is generated to increase the user's risk score. An event to increase the score is also sent when a new internal destination port is used by the user.

Event name (new activity)

UBA : First time access to internal destination port

Event Name (activity deviation)

UBA : Increased activity to internal destination port

sensevalue

5

Required configuration

Configure the Network Hierarchy to help with the accuracy of determining internal destination ports.

Log source types

All events that have a defined username and local destination port.

Lateral Movement : Network Zone Activity

The *Lateral Movement : Network Zone Activity* model determines if a user's network zone is significantly different from the user's defined group.

Enable the *Lateral Movement : Network Zone Activity* model to determine if a user's network zone is significantly different from the user's defined group. If the user's activity is significantly different from the user's defined group, it is deemed suspicious and a Sense Event is generated to increase the user's risk score.

Event name (new activity)

UBA : First time access to network zone

Event Name (activity deviation)

UBA : Unusual network zone access

sensevalue

5

Required configuration

Configure the Network Hierarchy to help with the accuracy of determining network zones.

Log source types

All events that have a defined username and local destination IP.

Process Usage

The *Process Usage* model tracks a user's process usage activity in time and creates a model for the predicted weekly behavior patterns.

Enable the *Process Usage* model to track a user's process usage activity in time and create a model for the predicted weekly behavior patterns. If the user's activity deviates from the learned behavior, it is deemed suspicious and a Sense Event is generated to increase the user's risk score. An event to increase the score is also sent when a new process is used by the user.

Event name (new activity)

UBA : User running new process

Event Name (activity deviation)

UBA : Increase in process usage

sensevalue

5

Required configuration

The *Process Name* property must be defined.

Log source types

Looks at events that have the *Process Name* property defined for it.

Peer group models

Peer group models calculate a set of attributes with their corresponding event count numeric value for the user for the past 30 days. The ML model determines with a high level of confidence that the user deviated outside of the group.

Related concepts

[Individual \(Numeric\) user models](#)

Individual (Numeric) user models calculate a specific numeric value for the user for the past 10 days. When the user deviates outside of the predicted range, the Machine Learning model determines with a high level of confidence that the event is anomalous.

[Individual \(Observable\) user models](#)

Individual (Observable) user models calculate a set of attributes and their corresponding event count for the user for the past 10 days. When the user deviates outside the predicted range or uses a new value, the ML model determines with a high level of confidence that the event is anomalous.

[Machine learning analytic requirements](#)

Machine learning models can take some time to train and build based on different analytic requirements.

Related tasks

[Creating a custom model](#)

Create a custom model to measure and baseline a numeric feature for a person per hour.

[Peer group model grouping requirements](#)

Peer group machine learning models require grouping properties to meet minimum requirements.

Activity Distribution

The *Activity Distribution* model learns behavior clusters based on LDAP group definition and searches for deviations from the normal distribution of these clusters over time.

Enable the *Activity Distribution* machine learning model to display dynamic behavior clusters for all users that are monitored by machine learning on the **User Details** page. Malicious behavior can manifest as changes in the distribution of a user's behavior cluster; that is, the user's activities begin to deviate from his customary activities. Similar activities are represented by the same colors for all users. Starting with 4.0.0, users are grouped and analyzed based on the **Group by** field.

Important: You must have a minimum of two defined groups that each contains 5 or more users. If you change the group selection, a new model needs to be constructed. A significant amount of time and computer resources are required to complete the model creation. It is not recommended to change this value frequently.

Event name

UBA : Deviation from normal activity patterns

sensevalue

5

Required configuration

Select a group from the group by field, such as job title, department, or custom group in order to enable the model. Groups are defined in the user import tuning configuration originating from the user import data. For more information, see [“Tuning user import configurations” on page 41](#).

Log source types

Any log source with events that provide a username.

Defined Peer Group

The *Defined Peer Group* model shows how much a user's event activity deviates from the event activity of their defined peer group.

Enable the *Defined Peer Group* model to display how much a user's event activity deviates from the event activity of their defined peer group on the **User Details** page. Users are grouped and analyzed based on the **Group by** field. If a user's current behavior is significantly different from the user's defined group, it is deemed suspicious and a Sense Event is generated to increase the user's risk score.

Important: You must have a minimum of two defined groups that each contains 5 or more users. If you change the group selection, a new model needs to be constructed. A significant amount of time and computer resources are required to complete the model creation. It is not recommended to change this value frequently.

Event name

UBA : Deviation from define peer group

sensevalue

5

Required configuration

Select a group from the group by field, such as job title, department, or custom group in order to enable the model. Groups are defined in the user import tuning configuration originating from the user import data. For more information, see [“Tuning user import configurations” on page 41](#).

You must have 7 days of event data available for the analytic to generate a model.

Log source types

Any log source with events that provide a username.

Internal Asset Access by Peer Group

The *Internal Asset Access by Peer Group* model determines if a user's internal asset access is significantly different from the user's defined group.

Enable the *Internal Asset Access by Peer Group* model to determine if a user's internal asset access is significantly different from the user's defined group. If the internal asset access is significantly different, it is deemed suspicious and a Sense Event is generated to increase the user's risk score. Users are grouped and analyzed based on the **Group by** field.

Important: You must have a minimum of two defined groups that each contains 5 or more users. If you change the group selection, a new model needs to be constructed. A significant amount of time and computer resources are required to complete the model creation. It is not recommended to change this value frequently.

Event name

UBA : Internal asset access deviation from peer group

sensevalue

5

Required configuration

Select a group from the group by field, such as job title, department, or custom group in order to enable the model. Groups are defined in the user import tuning configuration originating from the user import data. For more information, see [“Tuning user import configurations” on page 41](#).

Configure the Network Hierarchy to help with the accuracy of determining internal destination addresses.

Log source types

All events that have a defined username and local destination IP.

Internal Destination Ports by Peer Group

The *Internal Destination Ports by Peer Group* model determines if a user's access to internal destination ports is significantly different from that user's defined group. If the user's access is deemed suspicious, a Sense Event is generated to increase the user's risk score.

Enable the *Internal Destination Ports by Peer Group* to determine if a user's access to internal destination ports is significantly different from that user's defined group. If a user's access to internal destination ports is significantly different from the user's defined group, it is deemed suspicious and a Sense Event is generated to increase the user's risk score. Users are grouped and analyzed based on the **Group by** field.

Important: You must have a minimum of two defined groups that each contains 5 or more users. If you change the group selection, a new model needs to be constructed. A significant amount of time and computer resources are required to complete the model creation. It is not recommended to change this value frequently.

Event name

UBA : Abnormal usage of internal destination port for peer group

sensevalue

5

Required configuration

Select a group from the group by field, such as job title, department, or custom group in order to enable the model. Groups are defined in the user import tuning configuration originating from the user import data. For more information, see [“Tuning user import configurations” on page 41](#).

Configure the Network Hierarchy to help with the accuracy of determining internal destination ports.

Log source types

All events that have a defined username and local destination port.

Learned Peer Group

The *Learned Peer Group* model identifies users who engage in similar activities and then places them into peer groups.

Enable the *Learned Peer Group* model to display how much the user deviated from the inferred peer group that they were expected to be in on the **User Details** page. If a user's current peer group is significantly different from former groups, then a Sense Event is generated to increase the user's risk score.

Event name

UBA : Deviation from learned peer group

sensevalue

5

Required configuration

Select a group from the group by field, such as job title, department, or custom group in order to enable the model. Groups are defined in the user import tuning configuration originating from the user import data. For more information, see [“Tuning user import configurations” on page 41](#).

To enable the *Learned Peer Group* model on QRadar 7.4.3 and later, you must install an App Host. For more information, see [App Hosts](#).

You must have 7 days of event data available for the *Learned Peer Group* analytic to generate a model.

Log source types

Any log source with events that provide a username.

Network Zones by Peer Group

The *Network Zones by Peer Group* model determines if a user's network zone is significantly different from that user's defined group.

Enable the *Network Zones by Peer Group* to determine if a user's network zone is significantly different from the user's defined group. If the user's network zone is deemed suspicious, a Sense Event is generated to increase the user's risk score. Users are grouped and analyzed based on the **Group by** field.

Important: You must have a minimum of two defined groups that each contains 5 or more users. If you change the group selection, a new model needs to be constructed. A significant amount of time and computer resources are required to complete the model creation. It is not recommended to change this value frequently.

Event name

UBA : Unusual network zone access for peer group

sensevalue

5

Required configuration

Select a group from the group by field, such as job title, department, or custom group in order to enable the model. Groups are defined in the user import tuning configuration originating from the user import data. For more information, see [“Tuning user import configurations” on page 41](#).

Configure the Network Hierarchy to help with the accuracy of determining internal destination ports.

Log source types

All events that have a defined username and local destination IP.

Process Execution by Peer Group

The *Process Execution by Peer Group* model determines if a user's process usage is significantly different from the user's defined group.

Enable the *Process Execution by Peer Group* model to determine if a user's process usage is significantly different from the user's defined group. If a user's process usage is significantly different from the user's

defined group, it is deemed suspicious and a Sense Event is generated to increase the user's risk score. Users are grouped and analyzed based on the **Group by** field.

Important: You must have a minimum of two defined groups that each contains 5 or more users. If you change the group selection, a new model needs to be constructed. A significant amount of time and computer resources are required to complete the model creation. It is not recommended to change this value frequently.

Event name

UBA : Abnormal process execution for peer group

sensevalue

5

Required configuration

Select a group from the group by field, such as job title, department, or custom group in order to enable the model. Groups are defined in the user import tuning configuration originating from the user import data. For more information, see [“Tuning user import configurations” on page 41](#).

You must define the *Process Name* property.

Log source types

Looks at events that have the *Process Name* property defined for it.

Creating a custom model

Create a custom model to measure and baseline a numeric feature for a person per hour.

Before you begin

Review the following model details for each model template:

- [Application Events](#)
- [Source IP](#)
- [Destination Port](#)
- [Office File Access](#)
- [AWS Access](#)
- [Process](#)
- [Website](#)
- [Risky IP](#)

About this task

You can create a custom model so that you can review the learned behavior and the actual data for users. If significant changes from the baseline behavior are detected, you will receive alerts that the user's risk score is raised. Examples of models you can create include: showing how much data a user downloads, how many applications a user runs, or how many emails a user send per hour.



Attention: After you configure or modify your settings, it takes a minimum of 1 hour to ingest data, build an initial model, and see initial results for users.

Active users are monitored continuously. If a user has no activity for 28 days, the user and the user's data are removed from the model. If the user is active again, they will return as a new user.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. Click **Apps > User Entity Analytics > Machine Learning Settings**.
3. On the **Machine Learning Settings** page, click **Create Model**.
4. On the **Model Definition** tab, you can select a template to populate the AQL field or you can create a custom AQL query.
5. Click **Next**.

Create Model

Enabled: No

Model Definition General Settings

Define a new model by choosing a template or by creating your own custom AQL query.

Select a template (optional) ▼

Custom AQL query i

Define the query that is used to populate the ML model. There are three parts to the query:

- The property whose value is used to build the model.
- The AQL function that is applied to the field. The model aggregates multiple events over a specific time period.
- A filter component that can be used to restrict the scope of the model to specific data

Property * i

Function * i

AQL search filter i

```
Example filter:  
{LOGSOURCETYPENAME(devicetype) = 'Linux  
OS'}
```

Summary: This models the **[Function]** of the field **[Property]** for users each hour.

6. On the **General Settings** tab, enter a name and description.
7. In the **Risk value of sense event** field, enter the amount to increase the user's risk score when a sense event is triggered. The default value is 5.
8. Enable the toggle to scale the risk value. When enabled, the base risk value is multiplied by a factor (range 1 - 10). This factor is determined by how much the user deviates from their expected behavior and not just that they deviated.

9. In the **Confidence interval to trigger anomaly** field, enter the percentage for how confident the machine learning algorithm should be before it triggers an anomalous event. The default value is 0.95.
10. In the **Data Retention Period** field, set the number of days you want to save the model data. The default value is 30.
11. The **Show graph on User Details page** toggle is disabled by default. If you want to display the custom model graph on the **User Details** page, click the toggle.
12. In the **AQL Search Filter** field, you can add an AQL filter to narrow the data that the analytic queries for in QRadar. By filtering with an AQL query, you can reduce the number of users or the types of data the analytic is analyzing. Before you save your settings, click **Validate Query** to launch a full AQL query in QRadar so that you can review the query and verify the results.

Important: If you modify the AQL filter, the existing model is marked invalid and is then rebuilt. The length of time the rebuild takes depends on the amount of data that is returned by the modified filter.

You can filter on specific log sources, network names, or reference sets that contain specific users. See the following examples:

- **REFERENCESETCONTAINS('Important People', username)**
- **LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')**
- **INCIDR('172.16.0.0/12', sourceip) or INCIDR('10.0.0.0/8', sourceip) or INCIDR('192.168.0.0/16', sourceip)**

For more information, see [Ariel Query Language](#).

13. Click **Save**.

✕
Create Model

Enabled: No

Model Definition
General Settings

Name * i

Description

Risk value of sense event * i

Scale risk value i

Confidence level to trigger anomaly * i

Data retention period * i

Show graph on user details page i

Enter a description

Cancel

Previous

Save

Related concepts

[Individual \(Numeric\) user models](#)

Individual (Numeric) user models calculate a specific numeric value for the user for the past 10 days. When the user deviates outside of the predicted range, the Machine Learning model determines with a high level of confidence that the event is anomalous.

[Individual \(Observable\) user models](#)

Individual (Observable) user models calculate a set of attributes and their corresponding event count for the user for the past 10 days. When the user deviates outside the predicted range or uses a new value, the ML model determines with a high level of confidence that the event is anomalous.

[Peer group models](#)

Peer group models calculate a set of attributes with their corresponding event count numeric value for the user for the past 30 days. The ML model determines with a high level of confidence that the user deviated outside of the group.

Machine learning analytic requirements

Machine learning models can take some time to train and build based on different analytic requirements.

Related tasks

Peer group model grouping requirements

Peer group machine learning models require grouping properties to meet minimum requirements.

Application Events

Procedure

- Event Name: UBA : Custom Analytic Anomaly
- senseValue = 5
- Required configuration: System is monitoring events that have QRadar high level category of Application.
- Log source types: APC UPS, Apache HTTP Server, Application Security DbProtect, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Web Application Firewall, Barracuda Web Filter, Blue Coat Web Security Service, BlueCat Networks Adonis, CRE System, Centrifry Infrastructure Services, Check Point, Cilasoft QJRN/400, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco FireSIGHT Management Center, Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco Meraki, Cisco Nexus, Cisco PIX Firewall, Cisco Stealthwatch, Cisco Umbrella, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, Custom Rule Engine, Cyber-Ark Vault, DG Technology MEAS, EMC VMWare, Event CRE Injected, Extreme Matrix K/N/S Series Switch, Extreme Stackable and Standalone Switches, F5 Networks BIG-IP AFM, F5 Networks BIG-IP ASM, F5 Networks BIG-IP LTM, Fidelis XPS, FireEye, Flow Classification Engine, Flow Device Type, Forcepoint Sidewinder, Forcepoint V Series, Fortinet FortiGate Security Gateway, FreeRADIUS, H3C Comware Platform, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM DB2, IBM DataPower, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM Resource Access Control Facility (RACF), IBM Security Directory Server, IBM Tivoli Access Manager for e-business, IBM i, IBM z/OS, ISC BIND, Imperva SecureSphere, Infoblox NIOS, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks AVT, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper WirelessLAN, Kisco Information Systems SafeNet/i, Linux DHCP Server, McAfee Network Security Platform, McAfee Web Gateway, Metainfo MetaIP, Microsoft DHCP Server, Microsoft DNS Debug, Microsoft Exchange Server, Microsoft IIS, Microsoft Office 365, Microsoft Operations Manager, Microsoft Windows Security Event Log, Motorola SymbolAP, NGINX HTTP Server, Nortel Contivity VPN Switch, Nortel VPN Gateway, OS Services Qidmap, OSSEC, ObserveIT, Okta, Open LDAP Software, OpenBSD OS, Oracle BEA WebLogic, Oracle Database Listener, PostFix MailTransferAgent, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware DefensePro, SSH CryptoAuditor, Skyhigh Networks Cloud Security Platform, Solaris Operating System Authentication Messages, Solaris Operating System DHCP Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Sophos Web Security Appliance, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sun ONE LDAP, Symantec Critical System Protection, Symantec Encryption Management Server, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), Top Layer IPS, Trend InterScan VirusWall, Trend Micro Deep Security, Universal DSM, Venustech Venusense Security Platform, Verdasys Digital Guardian, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

SourceIP

Procedure

- Event Name: UBA : Custom Analytic Anomaly
- sensevalue: 5
- Log source types: Any log source that contains username and source ip in the events.

Destination Port

Procedure

- Event Name: UBA : Custom Analytic Anomaly
- sensevalue: 5
- Log source types: Any log source that contains username and destination port in the events

Office File Access

Procedure

- Event Name: UBA : Custom Analytic Anomaly
- sensevalue: 5
- Required configuration : System is monitoring event that have QRadar event names that include the word "file".
- Log source type: Microsoft Office 365

AWS Access

Procedure

- Event Name: UBA : Custom Analytic Anomaly
- sensevalue: 5
- Required configuration: System is monitoring events that contain QRadar event names that include the word "bucket".
- Log source types: Amazon AWS Cloudtrail

Process

Procedure

- Event Name: UBA : Custom Analytic Anomaly
- sensevalue: 5
- Required configuration: Custom event property 'Process' must exist for the desired log source type.
- Log source types: Microsoft Windows Security Event Log; Linux OS

Website

Procedure

- Event Name: UBA : Custom Analytic Anomaly
- sensevalue: 5

- Support rules: 'UBA : Browsed to Entertainment Website', 'UBA : Browsed to LifeStyle Website', 'UBA : Browsed to Business/Service Website', 'UBA : Browsed to Communications Website'
- Required configuration: Custom event property 'Web Category' must exist for the desired log source type.
- Log source types: Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series; Forcepoint V Series, Fortinet FortiGate Security Gateway

Risky IP

Procedure

- Event Name: UBA : Custom Analytic Anomaly
- sensevalue: 5
- Required configuration: Set "Enable X-Force Threat Intelligence Feed" to Yes in **Admin Settings > System Settings**.
- Log source types: Any log source with events that have a user name.

Peer group model grouping requirements

Peer group machine learning models require grouping properties to meet minimum requirements.

About this task

To view a peer group model, you must configure user imports (**Admin Settings > User Entity Analytics > User Import**) to gather user grouping properties to meet minimum requirements. Select the grouping property on the configuration page that represents the groups to be modeled. See [Tuning user import configurations](#) for details on configuring the custom group.

You must have a minimum of two defined groups that each contains 5 or more users. If you change the group selection, a new model needs to be constructed. A significant amount of time and computer resources are required to complete the model creation. You should not change this value frequently.

Related concepts

[Individual \(Numeric\) user models](#)

Individual (Numeric) user models calculate a specific numeric value for the user for the past 10 days. When the user deviates outside of the predicted range, the Machine Learning model determines with a high level of confidence that the event is anomalous.

[Individual \(Observable\) user models](#)

Individual (Observable) user models calculate a set of attributes and their corresponding event count for the user for the past 10 days. When the user deviates outside the predicted range or uses a new value, the ML model determines with a high level of confidence that the event is anomalous.

[Peer group models](#)

Peer group models calculate a set of attributes with their corresponding event count numeric value for the user for the past 30 days. The ML model determines with a high level of confidence that the user deviated outside of the group.

[Machine learning analytic requirements](#)

Machine learning models can take some time to train and build based on different analytic requirements.

Related tasks

[Creating a custom model](#)

Create a custom model to measure and baseline a numeric feature for a person per hour.

Machine learning analytic requirements

Machine learning models can take some time to train and build based on different analytic requirements.

Machine learning analytics

- **Peer group analytics:** These analytics identify users who engage in similar activities and the model places them into peer groups. Alerts are then generated based on deviations from a user from their peer group.

Peer Group models do not have a training phase. They have only a model building phase and a scoring phase because they ingest back 30 days of a user's data.

- **HOURLY_WINDOW Analytics:** The model is cumulative, so each hour is evaluated against the model for each user as a whole as opposed to having its own model.

The hours to train this type of model are written as real-world hours. For example, 240 hours of data needed would mean that 10 days or 240 real-world hours would need to elapse.

- **HOURLY_HOUR Analytics:** These analytics build a model for each user for each of the hours of the day. For example, there will be a 1 PM – 2 PM model, a 2 PM – 3 PM model and so on.

The hours required to train are written as hours for each model. For example, 10 hours of data needed would mean that 10 days or 240 real-world hours need to elapse.

Analytic terminology

- **minTimeSpan:** This is the model's minimum required number of hours to be able to train and build.
- **ticketMinSampleCounts:** This differs from minTimeSpan as it's the minimum number of hours that are needed to generate alerts. Peer Group Analytics do not have this parameter.
- **Number of roles:** The minimum number of roles and the maximum number of roles are a range that the model tests for each and every number in that range to determine how many clusters of low-level categories to segment users into. The model evaluates each number of clusters within the range and determines what number of topics is optimal.

Peer group analytics

The following models use Peer group analytics:

- Activity Distribution
- Defined Peer Group
- Internal Asset Access by Peer Group
- Internal Destination Port by Peer Group
- Internal Network Zone by Peer Group
- Learned Peer Group
- Process Execution by Peer Group

These are the parameters for a peer group model to build:

- Type of analytic: Peer Group
- Minimum number of roles: 2
- Maximum number of roles: 13

Note: Learned Peer Group, Defined Peer Group, and Activity Distribution all have a maximum of 20

- Minimum number of groups: 5
- Maximum number of groups: 10

Note: Learned Peer Group is the only one with a maximum of 20.

- Minimum number of events: 10
- Minimum amount of data to build (mintimespan): 7 Days
- Current set amount of data to build (timespan): 30 Days

HOURLY_TO_WINDOW analytics

The following models use HOURLY_TO_WINDOW analytics:

- DDL Events
- DML Events
- Inbound Data Transfer
- Internal Asset Access
- Internal Destination Port
- Internal Network Zone
- Large HTTP Transfer
- Outbound Transfer Attempts
- Outbound Transfer Attempts (by Volume)
- Process Usage
- Risk Posture
- Successful Access and Authentication Activity

These are the parameters for an HOURLY_TO_WINDOW model to build:

- Type of analytic: HOURLY_TO_WINDOW
- Minimum amount of data to build (mintimespan): 240 Hours
- Minimum amount of data to generate alerts (ticketMinSampleCounts): 240 Hours
- Current set amount of data to build (timespan): 240 Hours
- SenseValue: 5

HOURLY_TO_HOUR analytics

The following models use HOURLY_TO_HOUR analytics:

- Aggregated Activity
- Access Activity
- Authentication Activity
- Suspicious Activity

These are the parameters for an HOURLY_TO_HOUR model to build:

- Type of analytic: HOURLY_TO_HOUR
- Minimum amount of data to build (mintimespan): 240 Hours
- Current set amount of data to build (timespan): 240 Hours
- Minimum amount of data to generate alerts (ticketMinSampleCounts): 10 Hours (10 real-world days)

Related concepts

Individual (Numeric) user models

Individual (Numeric) user models calculate a specific numeric value for the user for the past 10 days. When the user deviates outside of the predicted range, the Machine Learning model determines with a high level of confidence that the event is anomalous.

Individual (Observable) user models

Individual (Observable) user models calculate a set of attributes and their corresponding event count for the user for the past 10 days. When the user deviates outside the predicted range or uses a new value, the ML model determines with a high level of confidence that the event is anomalous.

Peer group models

Peer group models calculate a set of attributes with their corresponding event count numeric value for the user for the past 30 days. The ML model determines with a high level of confidence that the user deviated outside of the group.

Related tasks

Creating a custom model

Create a custom model to measure and baseline a numeric feature for a person per hour.

Peer group model grouping requirements

Peer group machine learning models require grouping properties to meet minimum requirements.

Chapter 11. Troubleshooting and support

To isolate and resolve problems with your IBM product, you can use the troubleshooting and support information.

For answers to common support questions about the IBM QRadar User Entity Behavior Analytics app and the Machine Learning Analytics app, see <https://developer.ibm.com/answers/topics/uba/>

Help and support page for UEBA

The User Entity Behavior Analytics (UEBA) app includes a Help and Support section for using the UEBA app and the Machine Learning Analytics (ML) app.

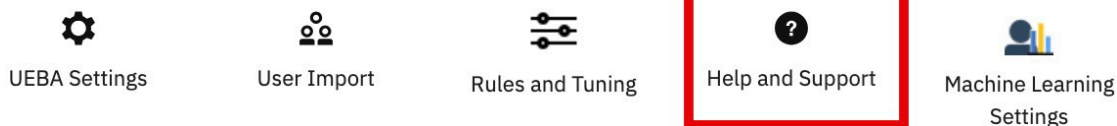
Accessing the Help and Support page for UEBA

The **Help and Support** page provides links to documentation, education, log files, and administrative functions. You must have QRadar administrator privileges to view log files and complete administrative functions from the **Help and support** page.

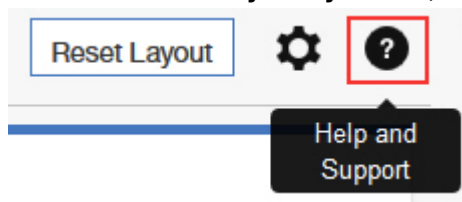
After you install the UEBA app, you can access the **Help and Support** page from the following locations:

- From the Admin Settings, click **Apps > User Entity Analytics > Help and Support**.

User Entity Analytics



- From the **User Entity Analytics** tab, click the **Help and Support** icon.



Administrative functions

You must have QRadar administrator privileges to view log files and complete administrative functions.

Administrative functions include the ability to complete the following actions:

- Click **Clear UBA Data** to remove all UEBA user data but maintain all of your current UEBA configuration settings. Clearing UEBA data makes the UEBA app behave as if you just installed and configured the **UBA Settings**. If the Machine Learning (ML) app is installed, the **Clear UBA Data** button also resets the ML app.

Note: When you click **Clear UBA Data** to remove all users from the UEBA database, it is possible for some or all of the users to immediately appear in the UEBA database if those users have received a QRadar event within the last hour that has a senseValue score associated with it.

- Click **Remove event users** to remove users that were discovered through events. You can click the number link to go to the search page that shows the list of users that will be deleted. After confirming

the user removal, the count on the overview page under Users discovered from events should decrease to zero. Users that were imported are not affected and will not be removed. Tip: You should enable the **Monitor imported users only** option on the UEBA Settings page before removing event users if you don't want to discover users from events again. Note: If there are no event users, this option will be hidden.

- Click **Remove users without aliases** to delete the user record from the database.
Important: This option only appears if there are users without aliases in your database.
- Click **Reset ML Settings** if the ML app is installed and you want to reset all of your Machine Learning settings and disable all of the analytics that are enabled.

Service requests

Service requests are also known as Problem Management Records (PMRs).

Several methods exist to submit diagnostic information to IBM Software Technical Support. To open a service request, or to exchange information with technical support, view the IBM Software Support Exchanging information with Technical Support page (<http://www.ibm.com/software/support/exchangeinfo.html>). Service requests can also be submitted directly by using the Service requests (PMRs) tool (http://www.ibm.com/support/entry/portal/Open_service_request).

Machine Learning supervisorctl status shows EXITED

If postconfigs in the supervisorctl status of machine learning shows EXITED, no action is required.

The process of **Postconfigs** in **supervisorctl status** shows **EXITED**. This is expected behavior. Postconfigs only run during a fresh installation or upgrade of UEBA.

Machine Learning app status shows warning on dashboard

If the Status of machine learning models on the UEBA dashboard shows warning messages, review the procedures to resolve the issue.

If the Status of machine learning models shows **Model failed to build**, you can try the following suggestions to resolve the issue:

- See the error logs for the ML app.
- Check the disk space on the system that is running the ML app.
- Verify that the UEBA app has users with events.
- Contact IBM Customer Support.

Related concepts

[“Downloading UEBA and Machine Learning logs” on page 276](#)

Use the UEBA and Machine Learning log files to help troubleshoot problems.

Machine Learning status shows no progress for data ingestion

If the Status of machine learning models on the UEBA dashboard appears to be stuck during the data ingestion phase, review the procedure to resolve the issue.

If the Status of machine learning models shows no progress for data ingestion for an analytic, you can try the following suggestions to resolve the issue:

- Restart the Ariel Server Service
- Check the disk space on the system running the ML app.
- Check inside the ML container to see if the **UBAController** process is running.
- Contact IBM Customer Support.

ML app status is in an error state

If the Machine Learning Analytics (ML) app fails to install and the Machine Learning Settings shows an Error status, you can use the **cURL** command line tool and the API Documentation settings to uninstall the ML app.

Procedure





If the Machine Learning Analytics (ML) App Status in the Machine Learning Settings page shows Error, complete the procedure to uninstall the failed app.

Machine Learning Settings

Setting up the Machine Learning Analytics (ML) App

1. Install and configure the User Behavior Analytics (UBA) app.
2. Verify the UBA app has polled once and that there is user data present.
3. Install proper version of the Machine Learning Analytics app. See the table for matching versions.
4. Return to the Machine Learning Analytics Configuration page to configure the Machine Learning Analytics app.

ML APP Requirement Checks

Check	Current	Required	Status
QRadar Version	7.2.8	7.2.7+	
Security Token	Configured	Configured	
Available Memory	12 GB	5 GB	
ML App Status	Error	Running	

Note: You must have a valid authentication token. You can see the list of configured authentication tokens in the Authorized Services section in the Admin settings of the QRadar Console.

1. Using SSH, log in to the QRadar Console.
2. Run the following command:

```
# psql -U qradar -c 'select id,name,status from installed_application'
```

Example output:

```
id | name | status
-----+-----+-----
1356 | User Entity Analytics | RUNNING
1358 | Machine Learning Analytics | ERROR
1357 | dataimport.ldap.applicationname | RUNNING
```

3. Locate and record the *id* value for Machine Learning Analytics from the output of the command.
4. Using a valid authentication token in the place of *<valid token>* and the recorded *id* value in place of *<id>*, run the following command to uninstall the failed Machine Learning app: **# curl -X DELETE -k -H 'SEC:<valid token>' https://127.0.0.1/api/gui_app_framework/applications/<id>**

Removing the Machine Learning app

To remove the Machine Learning app using the `gui_app_framework` API, complete the following steps:

1. Open the QRadar Console and navigate to the API doc page at the following location: `https://<host_address_port>/api_doc`
2. Open the folder for the highest API version number (the number is different based on the QRadar version; for example, 7.0 on QR 7.2.8).
3. Open the `/gui_app_framework` folder and then select `/applications`.
4. At this point, you should be at the **GET API**. Click the **"Try It Out!"** button to get the list of installed applications.
5. Search for `Machine Learning Analytics` in the results from step 4 and get the `application_id` attribute value.
6. Expand the `/applications` menu in the API docs (same location as step 3), select the `/application_id` API and click the **DELETE** tab.
7. Enter the application ID value from step 5 and then click the **"Try It Out!"** button to remove the application.
8. The API should return an HTTP 204 status code to indicate the application was successfully removed.

Downloading UEBA and Machine Learning logs

Use the UEBA and Machine Learning log files to help troubleshoot problems.

Downloading app log files

You can download log files for the UEBA app and the Machine Learning (ML) app from the ["Help and support page for UEBA"](#) on page 273.

The screenshot shows a dark blue header with the text "Help and Support". Below the header, there are three main sections:

- Useful Links**:
 - [UEBA user guide \(online\)](#)
 - [UEBA user guide \(download\)](#)
 - [IBM Security Learning Academy \(free courses on UEBA setup and features\)](#)
- App Logs**:
 - User Entity Behavior Analytics (UEBA)
 - [Download log files](#)
 - [Show all error messages in logs](#)
- Administrative Functions**:
 - [Clear UEBA Data](#) Clears user and entities data but maintains the current settings. This also resets the Machine Learning app.
 - [Remove event users](#) 8 UEBA monitored users that were discovered through events will be removed. This action does not affect imported users.

Chapter 12. APIs for UEBA

Use the APIs for UEBA.

Public API documentation for UEBA

You can gather information from the UEBA database with the public API documentation. Each endpoint targets certain users and returns data about them. All responses are in JSON syntax. These APIs rarely change. You can use the APIs to gather a snapshot of a user at a particular time to compare to a later date.

Required information

- SEC Token with UEBA capabilities referred to as SEC_TOKEN
- UEBA App ID referred to as UBA_APP_ID
- QRadar Console IP address, if scripts are not run locally, referred to as QR_IP_ADDRESS

User above threshold

The `users_above_threshold` API endpoint gathers users who are above the risk threshold. It returns the current risk score of the system and the users who risk is above the threshold. The user data returned has fields shown in the sample below from UBA database.

cURL command

```
curl -k -H 'Content-Type:application/json' -H 'Accept:application/json' -H 'SEC:SEC_TOKEN' https://QR_IP_ADDRESS/console/plugins/UBA_APP_ID/app_proxy/api/users_above_threshold
```

Sample return

```
{ "risk_threshold": 305.0, "users": [ { "alert": "Test", "aliases": [ "john.doe" ], "city": null, "country": null, "custom_group": null, "dept": null, "display_name": "john.doe", "email": null, "full_name": null, "id": 4, "id1": "john.doe", "id2": null, "id3": null, "id4": null, "in_custom_grp_peer_group_watchlist": false, "in_dept_peer_group_watchlist": false, "in_job_title_peer_group_watchlist": false, "in_ml_abridged_watch_list": true, "in_ml_watch_list": true, "in_peer_group_watchlist": false, "investigation_expires": 1626364130, "investigation_started": 1626277730, "investigation_user": "admin", "job_title": null, "last_offense_time": 1626275154, "latest_risk": 90.0, "linked_import_ids": null, "manager": null, "member_of": null, "ml_id": "john.doe", "ml_watched": false, "prolonged_risk": 21380.0, "risk": 1618.95, "risk_1": 1620.49, "risk_2": 1606.45, "risk_3": 1628.62, "risk_poll_count": 230, "risk_scale_max": 1.0, "source": "ariel", "state": null, "trending": -1, "trusted_user": false, "updated_this_run": 0, "username": "john.doe", "watched": 1, "watchlist_memberships": [ { "addition_date": 1626267571, "from_ref_set": false, "from_regex": true, "name": "Watch ML Users with data", "ref_set": null, "regex": "ibm_sense", "regex_field": "username", "risk_scale": 1.0, "source": "automatic", "watchlist_id": 2 } ], "watson_search_date": 0, "watson_search_id": null } ] }
```

User information

The `bulk_user_info` API endpoint gathers users who are specified in the list of users. It returns the current risk score of the system and the users who matches the name or names provided (case sensitive). The user data returned has fields shown in the following sample from the UBA database.

cURL command

```
curl -k -H 'Content-Type:application/json' -H 'Accept:application/json'
-H 'SEC:SEC_TOKEN' -X POST -d '{"users":["USER_NAME", "USER2_NAME",
"USER3_NAME"]}' https://QR_IP_ADDRESS/console/plugins/UBA_APP_ID/app_proxy/api/
bulk_user_info
```

Sample return

```
{
  "risk_threshold":244.0,
  "users": [
    {
      "alert":null,
      "alias_properties": [
        {
          "alias":"mike.smith",
          "is_dormant":false,
          "last_seen":0
        }
      ],
      "aliases": [
        "mike.smith"
      ],
      "city":null,
      "country":null,
      "custom_group":null,
      "dept":null,
      "display_name":"mike.smith",
      "email":null,
      "full_name":null,
      "id":3,
      "id1":"mike.smith",
      "id2":null,
      "id3":null,
      "id4":null,
      "in_custom_grp_peer_group_watchlist":false,
      "in_dept_peer_group_watchlist":false,
      "in_job_title_peer_group_watchlist":false,
      "in_ml_abridged_watch_list":true,
      "in_ml_watch_list":true,
      "in_peer_group_watchlist":false,
      "input_username":"mike.smith",
      "investigation_expires":0,
      "investigation_started":0,
      "investigation_user":null,
      "job_title":null,
      "last_offense_time":1626278817,
      "latest_risk":105.0,
      "linked_import_ids":null,
      "manager":null,
      "member_of":null,
      "ml_id":"mike.smith",
      "ml_watched":false,
      "prolonged_risk":21550.0,
      "risk":1642.33,
      "risk_1":1631.36,
      "risk_2":1612.69,
      "risk_3":1619.43,
      "risk_poll_count":235,
      "risk_scale_max":1.0,
      "source":"ariel",
      "state":null,
      "trending":1,
      "trusted_user":false,
      "updated_this_run":0,
      "username":"mike.smith",
      "watched":1,
      "watchlist_memberships": [
        {
          "addition_date":1626267571,
          "from_ref_set":false,
          "from_regex":true,
          "name":"Watch ML Users with data",
          "ref_set":null,
          "regex":"ibm_sense",
          "regex_field":"username",
          "risk_scale":1.0,
          "source":"automatic",
          "watchlist_id":2
        }
      ],
      "watson_search_date":0,
      "watson_search_id":null
    }
  ]
}
```

Investigated users

The `investigated_list` API endpoint gathers users who are currently under investigation. The user data returned has fields shown in the following sample from the UEBA database.

cURL command

```
curl -k -H 'Content-Type:application/json' -H 'Accept:application/json'
-H 'SEC:SEC_TOKEN' https://QR_IP_ADDRESS/console/plugins/UBA_APP_ID/app_proxy/api/
investigated_list
```

Sample return

Note: The following sample shows an example return of two users.

```
{
  "investigated": [
    {
      "alert":"Test",
      "aliases": [
        "john.doe"
      ],
      "color":"#A2191F",
      "color_severity":4,
      "display_name":"john.doe",
      "id":4,
      "investigation_user":"admin",
      "ml_id":"john.doe",
      "risk0":1674,
      "risk1":1663,
      "risk2":1667,
      "risk3":1688,
      "risk_scale_max":1,
      "score":1674.72,
      "trending":1
    },
    {
      "alert":null,
      "aliases": [
        "kelly.lin"
      ],
      "color":"#A2191F",
      "color_severity":4,
      "display_name":"kelly.lin",
      "id":33,
      "investigation_user":"admin",
      "ml_id":"kelly.lin",
      "risk0":307,
      "risk1":326,
      "risk2":345,
      "risk3":366,
      "risk_scale_max":1,
      "score":307.63,
      "trending":-1
    }
  ],
  "risk_threshold":244.0
}
```

Top 10 risky users

The `top_10_risky_users` API endpoint returns the top 10 riskiest users.

cURL command

```
curl -k -H 'Content-Type:application/json' -H 'Accept:application/json' -H 'SEC:SEC_TOKEN' https://QR_IP_ADDRESS/console/plugins/UBA_APP_ID/app_proxy/api/top_10_risky_users
```

Sample return

Note: The following sample only shows an example return of one user.

```
{
  "users": [
    {
      "alert": "Test",
      "aliases": [
        "john.doe"
      ],
      "city": null,
      "color_severity": 4,
      "country": null,
      "custom_group": null,
      "dept": null,
      "display_name": "john.doe",
      "email": null,
      "full_name": null,
      "id": 4,
      "id1": "john.doe",
      "id2": null,
      "id3": null,
      "id4": null,
      "in_custom_grp_peer_group_watchlist": false,
      "in_dept_peer_group_watchlist": false,
      "in_job_title_peer_group_watchlist": false,
      "in_ml_abridged_watch_list": true,
      "in_ml_watch_list": true,
      "in_peer_group_watchlist": false,
      "investigation_expires": 1626364130,
      "investigation_started": 1626277730,
      "investigation_user": "admin",
      "job_title": null,
      "last_offense_time": 1626278817,
      "latest_risk": 80.0,
      "linked_import_ids": null,
      "manager": null,
      "member_of": null,
      "ml_id": "john.doe",
      "ml_watched": false,
      "prolonged_risk": 22555.0,
      "risk": 1659.96,
      "risk_1": 1674.72,
      "risk_2": 1663.95,
      "risk_3": 1667.6,
      "risk_poll_count": 242,
      "risk_scale_max": 1.0,
      "source": "ariel",
      "state": null,
      "trending": -1,
      "trusted_user": false,
      "updated_this_run": 0,
      "user_id": 4,
      "username": "john.doe",
      "watched": 1,
      "watchlist_memberships": [
        {
          "addition_date": 1626267571,
          "from_ref_set": false,
          "from_regex": true,
          "name": "Watch ML Users with data",
          "ref_set": null,
          "regex": "ibm_sense",
          "regex_field": "username",
          "risk_scale": 1.0,
          "source": "automatic",
          "watchlist_id": 2
        }
      ],
      "watson_search_date": 0,
      "watson_search_id": null
    }
  ]
}
```

Top 10 anomalous users

The `top_ten_users_anomalies` API endpoint returns the 10 users with the most anomalies (rules fired).

cURL command

```
curl -k -H 'Content-Type:application/json' -H 'Accept:application/json' -H 'SEC:SEC_TOKEN' https://QR_IP_ADDRESS/console/plugins/UBA_APP_ID/app_proxy/api/top_ten_users_anomalies
```

Sample return

Note: The following sample shows an example return of one user.

```
{
  "users": [
    {
      "alert": "Test",
      "aliases": [
        "john.doe"
      ],
      "city": null,
      "color_severity": 4,
      "country": null,
      "custom_group": null,
      "dept": null,
      "display_name": "john.doe",
      "email": null,
      "full_name": null,
      "id": 4,
      "id1": "john.doe",
      "id2": null,
      "id3": null,
      "id4": null,
      "in_custom_grp_peer_group_watchlist": false,
      "in_dept_peer_group_watchlist": false,
      "in_job_title_peer_group_watchlist": false,
      "in_ml_abridged_watch_list": true,
      "in_ml_watch_list": true,
      "in_peer_group_watchlist": false,
      "investigation_expires": 1626364130,
      "investigation_started": 1626277730,
      "investigation_user": "admin",
      "job_title": null,
      "last_offense_time": 1626278817,
      "latest_risk": 80.0,
      "linked_import_ids": null,
      "manager": null,
      "member_of": null,
      "ml_id": "john.doe",
      "ml_watched": false,
      "prolonged_risk": 22830.0,
      "risk": 1652.54,
      "risk_1": 1666.13,
      "risk_2": 1660.97,
      "risk_3": 1659.96,
      "risk_poll_count": 245,

```

```
risk_scale_max":1.0,"source":"ariel","state":null,"total_anomalies":28,"trendin
g":-1,"trusted_user":false,"updated_this_run":0,"user_id":4,"username":"john.do
e","watched":1,"watchlist_memberships":
[{"addition_date":1626267571,"from_ref_set":false,"from_regex":true,"name":"Wat
ch ML Users with
data","ref_set":null,"regex":"ibm_sense","regex_field":"username","risk_scale":
1.0,"source":"automatic","watchlist_id":2}],{"watson_search_date":0,"watson_sear
ch_id":null}
```

Single user information

This API endpoint displays information for a single user.

cURL command

```
curl -k -H 'Content-Type:application/json' -H 'Accept:application/json' -H
'SEC:SEC_TOKEN' https://QR_IP_ADDRESS/console/plugins/UBA_APP_ID/app_proxy/api/
user_info?username=testUser
```

Sample return

```
{"display_name":"john.doe","id":4}
```

User risk score information

This API call displays a specific user risk score.

cURL command

```
curl -k -H 'Content-Type:application/json' -H 'Accept:application/json' -H
'SEC:SEC_TOKEN' https://QR_IP_ADDRESS/console/plugins/UBA_APP_id/app_proxy/api/
risk?username=testUser
```

Sample return

```
{"color":"#A2191F","color_severity":4,"id":4,"risk":1659.72}
```

UEBA generated offenses

This API call displays UEBA generated offenses.

cURL command

```
curl -k -H 'Content-Type:application/json' -H 'Accept:application/json' -H
'SEC:SEC_TOKEN' https://QR_IP_ADDRESS/console/plugins/UBA_APP_ID/app_proxy/api/
uba_offenses
```

Sample return

```
[ {"last_updated_time":1617736433612,"offense_id":699,"severity":6,"status":"OP
EN","user_id":79} ,
{"last_updated_time":1617732810616,"offense_id":860,"severity":7,"status":"OPEN
","user_id":252} ,
{"last_updated_time":1617728329632,"offense_id":881,"severity":8,"status":"OPEN
","user_id":264} ,
{"last_updated_time":1617724505250,"offense_id":693,"severity":6,"status":"OPEN
","user_id":113} ,
{"last_updated_time":1617719389070,"offense_id":876,"severity":7,"status":"OPEN
","user_id":165} ,
{"last_updated_time":1617719140504,"offense_id":795,"severity":6,"status":"OPEN
","user_id":232} ,
```

```
{ "last_updated_time": 1617717998609, "offense_id": 742, "severity": 8, "status": "OPEN", "user_id": 183 } ,  
{ "last_updated_time": 1617708897129, "offense_id": 749, "severity": 6, "status": "OPEN", "user_id": 77 } } ] Options
```

User import

Use the APIs to add directory server or reference table imports to the UEBA User Import feature.

Entry point

https://<<Qradar ip>>/console/plugins/<UBA app id>/app_proxy/user_import

Endpoints

HTTP Method	Endpoint	Media Type
POST	/cert	multipart/form-data
POST	/imports	application/json



ImportSchema ▾ {		
dataSource*	string <i>example: LDAP</i>	
		data source type, either LDAP or REF
configName*	string <i>example: My config 1</i>	
		the name for this import config
pollingInterval*	integer <i>example: 24</i>	
		the polling interval(in hours) to get the latest data from data source. The value should be 0 (manual poll) or 8 - 8640.
retrievalLimit*	integer <i>example: 500000</i>	
		the retrieval limit when polling data from data source. The value should 1 - 500,000
configLdap	LDAPConfigSchema ▾ {	
	description:	Connection and query configuration for directory server imports. Must be provided when dataSource is "LDAP".
ssl*	boolean <i>example: false</i>	Use ssl or not.
host*	string <i>example: example.com</i>	The host to connect LDAP with either hostname or IPv4.
port*	number <i>example: 389</i>	The port number to connect LDAP.
paged*	boolean <i>example: true</i>	Use paging or not.
baseDN*	string <i>example: dc=example,dc=com</i>	The base dn of the LDAP configuration.
filter*	string <i>example: (objectClass=person)</i>	The filter to query data from LDAP server.
username*	string <i>example:</i>	The username to access the LDAP server. Type "" if not provided.
password*	string(\$password) <i>example:</i>	The password to access the LDAP server. Type "" if not provided.

<p>ca*</p>	<p>caSchema {</p> <p>description:</p> <p>filename*</p> <p>expiryTime*</p>	<p>The file name and expiry time of the certificate associated with this import. You will get this information from the json response of the /cert API.</p> <p>string example: cert.pem</p> <p>The name of the certificate. Type "" if not provided.</p> <p>string example: Mon, 11 Jul 2039 03:37:19 GMT</p> <p>The expiry time of the certificate. Type "" if not provided.</p>
←		
<p>LDAPConfigSchema {</p> <p>description:</p> <p>ssl*</p> <p>host*</p> <p>port*</p> <p>paged*</p> <p>baseDN*</p> <p>filter*</p> <p>username*</p> <p>password*</p>	<p>Connection and query configuration for directory server imports. Must be provided when dataSource is "LDAP".</p> <p>boolean example: false</p> <p>Use ssl or not.</p> <p>string example: example.com</p> <p>The host to connect LDAP with either hostname or IPv4.</p> <p>number example: 389</p> <p>The port number to connect LDAP.</p> <p>boolean example: true</p> <p>Use paging or not.</p> <p>string example: dc=example,dc=com</p> <p>The base dn of the LDAP configuration.</p> <p>string example: (objectClass=person)</p> <p>The filter to query data from LDAP server.</p> <p>string example:</p> <p>The username to access the LDAP server. Type "" if not provided.</p> <p>string(\$password) example:</p> <p>The password to access the LDAP server. Type "" if not provided.</p>	

```

ca*
caSchema v {
  description:
    The file name and expiry time of the certificate associated with this import. You will get this information from the json response of the /cert API.

  filename*
    string
    example: cert.pem

    The name of the certificate. Type "" if not provided.

  expiryTime*
    string
    example: Mon, 11 Jul 2039 03:37:19 GMT

    The expiry time of the certificate. Type "" if not provided.

caSchema v {
  description:
    The file name and expiry time of the certificate associated with this import. You will get this information from the json response of the /cert API.

  filename*
    string
    example: cert.pem

    The name of the certificate. Type "" if not provided.

  expiryTime*
    string
    example: Mon, 11 Jul 2039 03:37:19 GMT

    The expiry time of the certificate. Type "" if not provided.

UploadCertSchema v {
  importId*
    integer
    example: 0

    The import ID for this certificate file. For new import, input 0.

  file*
    string($binary)

    The certificate file

```

Importing from an LDAP server with a certificate file

To import from an LDAP server with a certificate authority, complete the following steps.

1. Get the application UEBA app id by either going to UEBA Settings in the browser and looking at the URL in the address bar (between "plugins" and "app_proxy") or opening an SSH connection to the QRadar Console machine and issuing the following: **psql -U qradar -c "select id from installed_application where name = 'User Entity Analytics';"**

Note: You will use the application id when creating the URL used in the cURL commands.

2. If you want to create a new directory server import that uses a certificate, use the Cert API to upload the certificate file: **curl -X POST -F 'importId=0' -F 'file=@<PATH/TO/CERT/FILE>' -H "Content-Type: multipart/form-data" -H "SEC: <AUTHORIZED_SERVICE_TOKEN>" https://<QR_IP_ADDRESS>/console/plugins/<APP_ID>/app_proxy/user_import/cert**

Note: You will use the output of the cURL command in the body of the POST request that creates the new import.

3. Use the Imports API to create the new import
4. Enter the following command: **curl -X POST -H "Content-Type: application/json" -H "SEC: <AUTHORIZED_SERVICE_TOKEN>" -d '{"pollingInterval": 24,"configName": "<CONFIG_NAME>","retrievalLimit": 500000,"dataSource":"LDAP", "configLdap": {"filter": "(objectClass=person)", "ssl": false,"host": "<SERVER_IP_OR_HOSTNAME>","password": "", "username": "", "paged": true,"baseDN": "<BASE_DN>","ca": {"expiryTime": "<FROM_CERT_API>","filename": "<FROM_CERT_API>"},"port": 389}}' https://<QRADAR_IP_ADDRESS>/console/plugins/<APP_ID>/app_proxy/user_import/imports**

Importing from an LDAP server without a certificate file

To import from an LDAP server without a certificate file, complete the following steps.

1. Get the application UEBA app id by either going to UEBA Settings in the browser and looking at the URL in the address bar (between "plugins" and "app_proxy") or opening an SSH connection to

the QRadar Console machine and issuing the following: **psql -U qradar -c "select id from installed_application where name = 'User Entity Analytics';"**

Note: You will use the application id when creating the URL used in the cURL commands.

2. Use the Imports API to create the new import
3. Enter the following command: **curl -X POST -H "Content-Type: application/json" -H "SEC: <AUTHORIZED_SERVICE_TOKEN>" -d '{"pollingInterval": 24,"configName": "<CONFIG_NAME>","retrievalLimit": 500000,"dataSource":"LDAP", "configLdap": {"filter": "(objectClass=person)", "ssl": false,"host": "<SERVER_IP_OR_HOSTNAME>","password": "", "username": "", "paged": true,"baseDN": "<BASE_DN>","ca": {"expiryTime": "", "filename": ""}}, "port": 389}}' https://<QRADAR_IP_ADDRESS>/console/plugins/<APP_ID>/app_proxy/user_import/imports**

Importing from a reference table

To import from a reference table, complete the following steps

1. Get the application UEBA app id by either going to UEBA Settings in the browser and looking at the URL in the address bar (between "plugins" and "app_proxy") or opening an SSH connection to the QRadar Console machine and entering the following command: **psql -U qradar -c "select id from installed_application where name = 'User Entity Analytics';"**

Note: You will use the application id when creating the URL used in the cURL commands.

2. Most users choose to use the web interface to create a new reference table import. However, the Imports API is also supported.

Note: The reference table must already exist on the QRadar system and must be used as the CONFIG_NAME

3. Enter the following command: **curl -X POST -d '{"pollingInterval": 24, "configName": "<CONFIG_NAME>","retrievalLimit": 500000, "dataSource": "REF"}' -H "Content-Type:application/json" -H "SEC: <AUTHORIZED_SERVICE_TOKEN>" https://<QRADAR_IP_ADDRESS>/console/plugins/<APP_ID>/app_proxy/user_import/imports**

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions..

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

Trademarks

IBM, the IBM logo, and ibm.com[®] are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java[™] and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or

reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user’s session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at <http://www.ibm.com/privacy> and IBM's Online Privacy Statement at <https://www.ibm.com/privacy/details/us/en/> in the section entitled “Cookies, Web Beacons and Other Technologies”.

General Data Protection Regulation

Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients’ business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

To learn more about IBM's own GDPR readiness journey and our GDPR capabilities and offerings, see the following information: <https://ibm.com/gdpr>.

