



# QRadar Forum Migration & WinCollect

IBM SECURITY SUPPORT OPEN MIC

**Reminder:** You must dial-in to the phone conference to listen to the panelists.  
The web cast does not include audio.

USA toll-free: **866-803-2145**

USA toll: 1-210-795-1099

Participant passcode: **3192123**

Slides and additional dial in numbers: **<http://ibm.biz/forumswincollect>**

**NOTICE:** BY PARTICIPATING IN THIS CALL, YOU GIVE YOUR IRREVOCABLE CONSENT TO IBM TO RECORD ANY STATEMENTS THAT YOU MAY MAKE DURING THE CALL, AS WELL AS TO IBM'S USE OF SUCH RECORDING IN ANY AND ALL MEDIA, INCLUDING FOR VIDEO POSTINGS ON YOUTUBE. IF YOU OBJECT, PLEASE DO NOT CONNECT TO THIS CALL.

September 1, 2016



# Panelists

- Jamie Wheaton – Team Lead / Product Owner WinCollect
- Michael Hume – Team Lead, QRadar Integrations
- Chris Collins – QRadar Integration L3 Engineering
- Keith Degrace – Software Developer WinCollect
- Stephen Crawford – Software Engineer WinCollect
- Josh Ryan – Software Developer WinCollect
- Curt Wolfson – QRadar Support Knowledge Engineer

Presenter: Jonathan Pechta – Support Technical Writer / Support Content Lead

Moderator: Jack Cam – Support Manager

Assisting: Michael Hunt – Support Knowledge Co-op student



# Announcements



## QRadar 7.2.8 – Future API Changes

- QRadar 7.2.8 introduces V7.0 endpoints
- API 4.0 will be removed
- APIs 5.0 and 5.1 will be marked as deprecated

**Note:** A 2<sup>nd</sup> Open Mic event is scheduled for September 15<sup>th</sup> to discuss QRadar 7.2.8 features.

## QRadar Support Knowledgebase

- A new master tech note was released that contains links to all support content currently published. As we work on new articles, this page will be refreshed to include new content.

Where?

<http://ibm.biz/qradarknowledge>

### QRadar Knowledgebase Index

#### Question

Where can I find a list of all technotes relevant to QRadar?

#### Answer

The content below includes a list of all technical notes published under QRadar by category and sorted by popularity. documentation is released, this content will be updated and new articles added.

#### IBM Security QRadar SIEM

##### Expand All

- + --
- + Adaptive Log Exporter
- + Admin Console
- + Assets
- Dashboard

##### Doc Number ↕

##### Title ↕

<a href="#">1701213</a>	<a href="#">QRadar: X-Force Frequently Asked Questions (FAQ)</a>
<a href="#">1679314</a>	<a href="#">Sharing Dashboards Items from QRadar Saved Searches</a>
<a href="#">1683598</a>	<a href="#">QRadar: Threat Information Center Dashboard: XForce RSS Download Error</a>
<a href="#">1695099</a>	<a href="#">QRadar: How to create a dashboard for other users</a>
<a href="#">1671700</a>	<a href="#">Troubleshooting Managed Hosts that do not Display on the Dashboard EPS Graph</a>

- + Documentation
- + Flows
- + General Information
- + Hardware
- + High Availability
- + Installation



# Agenda



## QRadar 7.2.7 Feature Discussion Agenda

- Announcements
- QRadar Support Forum Migration
- WinCollect 7.2.4 Discussion
- Questions / general discussion



# Customer Support Forum Migration



# dW Answers – The new forum direction for QRadar Support

## Why the change?

- #1 answer is search performance and finding answers faster. In the existing forum, you had to search by forum group or use Google to search “QRadar developerworks <keywords>”. dW Answers has a global search that combines tags with keyword searches.
- IBM Security QRadar support is now focusing on dW Answers participation
- dW Answers uses a Q&A model, focused on finding answers to questions, rather than general discussion.
- More flexible
- More integrated
- More interactive
- More rewarding
- More responsive

The screenshot displays the dW Answers forum interface. At the top, there is a search bar with the text 'QRADAR' and a search icon. To the right of the search bar are options for 'Tags', 'Spaces', and 'More', along with an 'Ask a question' button. Below the search bar, the main content area is titled 'Questions tagged with "qradar"'. On the right side of this section, there are statistics: 'Following' (48 Posts, 25 Users, 4 Followers). Below the title, there are filters for 'All' and 'Unanswered', and a 'Sort by' dropdown menu with options 'Active', 'Newest', and 'Likes'. The list of questions includes:

- Why can't I find the commands in this technote in the related doc?**  
1 Answer, 0 Likes, 3 Views. Tags: TECHNOTE, QRADAR, SWG21989387. Answered by Jonathan.Pechta (IBM) on Sep 1, '16.
- QRadar AQL - sum over all rows?**  
0 Answers, 0 Likes, 4 Views. Tags: QRADAR, AQL, ADVANCED SEARCH. Asked by TobiasA (x) on Aug 31, '16.
- WinCollect 7.2.3 - Collected Windows Events - Cache - Max. File Size**  
1 Answer, 0 Likes, 19 Views. Tags: CACHE, QRADAR, COLLECTION, WINCOLLECT. Edited by Jonathan.Pechta (IBM) on Aug 30, '16.
- In QRadar, what is the file format for exporting the unknown log records**  
1 Answer, 0 Likes, 2 Views. Tags: EXPORT, QRADAR. Edited by Jonathan.Pechta (IBM) on Aug 30, '16.

On the right sidebar, there is a 'Topic experts' section featuring Jonathan.Pechta (IBM) with 135 points. Below that is a 'Related tags' section with various tags including TECHNOTE, EVENTS, XFORCE-EXCHANGE, IIB, PAYLOAD, SWG27048509, LOGGING, SWG21665955, SDK, SSL, APP, SITEPROTECTOR, TIME, EXTENSION, MAA S360, EXPORT, MAIL, INFORMATION-MANAGEMENT.

<https://ibm.biz/qradarforums> OR <https://developer.ibm.com/answers/questions/ask/?topics=qradar>



# dW Answers – Flexible


dW Answers uses tags to help categorize – flexible, simple, short, relevant, and easy to understand

<b>1</b> Answer	<b>0</b> Likes	<b>2</b> Views	<b>In QRadar, what is the file format for exporting the unknown log records</b>	<b>EXPORT</b> <b>QRADAR</b>	<i>Jonathan.Pechta (IBM) (151) edited   Aug 30, '16</i>
<b>1</b> Answer	<b>0</b> Likes	<b>54</b> Views	<b>How to create custom rules by using q-radar sdk</b>	<b>SDK</b> <b>QRADAR</b> <b>EXTENSION</b> <b>APP</b>	<i>Drew M (IBM) (100) answered   Aug 30, '16</i>
<b>1</b> Answer	<b>0</b> Likes	<b>25</b> Views	<b>What is the maximum event payload size of QRadar 7.2.6 using TCP syslog message?</b>	<b>EVENTS</b> <b>QRADAR</b> <b>TCP</b> <b>PAYLOAD</b>	<i>Jonathan.Pechta (IBM) (151) answered   Aug 16, '16</i>


<https://ibm.biz/qradarforums> OR <https://developer.ibm.com/answers/questions/ask/?topics=qradar>

# dW Answers – Integrated

Questions and comments on support content (tech notes & APARS) are not connected with dW Answers to get ask questions of information written by support teams.

 Be the first to ask a question

## QRadar: Changing the IMM networking configuration

 1 question - 1 answered

### Technote (FAQ)

#### Question

When first setting up Integrated Management Module (IMM) connectivity or making adjust configuration of the IMM.

#### Answer

**Quick Links:**

- [About IMM Network Configurations](#)

### Community questions and discussion

Ask a question about this topic. [Ask a question](#)

**Question:** I have immediate need of RHEL 7.x Client for the Guardium Data Encryption Agent. Is that supported?  
0 GDE  
votes By [restuser](#) on 08/02/2016 03:12 PM [Add your answer](#)

**Answer:**

According to the Compatibility Matrix posted at [support.vormetric.com](http://support.vormetric.com), support for various RHEL 7.x kernels started with agent version 5.2.3. What version/kernel of RHEL specifically?  
By [Matthew\\_Simons](#) on 08/03/2016 02:31 PM  
[Like](#) · [Comment](#) · [Share](#)

Answers | Was this answer helpful to you? [Yes](#) [No](#) [Report abuse](#)

**Question:** RHEL 7.1 Client  
0  
votes When is RHEL 7.1 client likely to be supported. We have an urgent need to deploy on RHEL 7.1. I can see the latest certified version is 6.3 but surely 7.1 should be fine?  
By [restuser](#) on 07/27/2016 11:32 AM [Add your answer](#)

**Answer:**

<https://ibm.biz/qradarforums> OR <https://developer.ibm.com/answers/questions/ask/?topics=qradar>

# dW Answers – Interactive

dW Answers offers a number of ways to work with the questions and answers

The screenshot illustrates the interactive features of dW Answers. It shows a question card for 'Guardium integration' with 1 answer, 0 likes, and 7 views. A 'TECHNOTE' tag is present, and a tooltip indicates 'This question has an accepted answer'. Below the question, there is a '1 reply · Add your answer' section with a profile picture and the text 'Accepted answer'. Interaction options include 'Like · 1', 'Comment', 'Reward user', and 'Share'. A 'Reward user' dialog box is open, allowing users to reward contributors with reputation points, with an input field for the number of points and a note that 88 points remain. The dialog has 'Cancel' and 'OK' buttons.

- Accept answers
- Like questions, answers, comments
- Reward contributors
- Share your findings

<https://ibm.biz/qadarforums> OR <https://developer.ibm.com/answers/questions/ask/?topics=qadar>


# dW Answers – Rewarding

dW Answers users gain Reputation, Followers, visibility

### Reward user

If you like this answer you can reward the user with reputation points.  
Use the input field to choose the number of points you would like to give.

Points:  (88 points remaining)



**5276**  
Reputation

**17**  
Followers

**0**  
Following

**85%**  
Accepted

Joined: Dec 02, 2013 at 03:31 PM  
Last seen: Aug 23 at 01:17 PM

### Top dW users



### My preferences

---

**Automatically-determined expertise:**  
Currently, you have not been automatically identified as an expert for any tags. dW Answers will automatically determine your expertise on a tag if you have enough positive activity in posts for that tag.

**Manually-added expertise:**  
You haven't manually added any expertise. Are you an expert in something? Let us know by adding tags.


<https://ibm.biz/qradarforums> OR <https://developer.ibm.com/answers/questions/ask/?topics=qradar>

# dW Answers – Responsive

- Use your normal IBM ID
- Follow specific tags
- Configure notifications

## dW Answers

Search  [Search tips](#) Tags ▾



**151** Reputation    **1** Followers    **2** Following    **0%** Accepted

Joined: May 21, 2014 at 12:36 PM  
Last seen: Sep 01 at 06:01 AM  
Display name: Jonathan.Pechta (IBM) [Change your display name](#)  
Email: Jonathan.Pechta@ca.ibm.com [Change your email address](#)

[Upload picture](#)    [Change your password](#)

### Jonathan.Pechta (IBM)

#### About me

IBM Technical Writer and Content Lead for everything QRadar related. I can take questions on any QRadar topic.

### General notifications:

A question is asked  None  Instantly  Daily  Weekly  
An answer is posted  None  Instantly  Daily  Weekly  
A comment is added  None  Instantly  Daily  Weekly  
A question in my area of expertise is asked  None  Instantly  Daily  Weekly  
A user follows me  None  Instantly  Daily  Weekly

### New activity in tags I follow:

A new question  None  Instantly  Daily  Weekly  
A new answer  None  Instantly  Daily  Weekly  
A question is edited  None  Instantly  Daily  Weekly  
A new comment  None  Instantly  Daily  Weekly  
A new accepted answer  None  Instantly  Daily  Weekly

### Auto subscriptions:

Questions I ask  Yes  No  
Questions I answer  Yes  No  
Questions I comment on  Yes  No  
Questions with tags I'm following.  Yes  No  
Questions in spaces I'm following.  Yes  No  
All new questions  Yes  No

### Additionally:

Notify me when someone replies to me using the @username notation  Yes  No  
Only use plain text when contacting me  Yes  No  
Send me a daily digest with unanswered questions  Yes  No

[Update settings](#) [Disable my notifications](#)

<https://ibm.biz/qradarforums> OR <https://developer.ibm.com/answers/questions/ask/?topics=qradar>

# dW Answers – Get involved!

- Ask questions
- Answer questions
- Share your expertise
- Call on other community members for help.

**Topic experts**

---

 You  
555 points

To reach out to another user via their user name, use @<username>

- You can use up to 8 tags in your question, however every tag must include QRadar.

**Required tag:** qradar

**Suggested addon tags:**

WinCollect,  
custom property,  
rules,  
troubleshooting,  
installation,  
etc

A larger number of tags exist in dW Answers already  
As you gain reputation, you can create your own tags.

## Ask a question



What is your question? Follow the tips below.

### Tips for asking questions

- Ask a question relevant to the dW Answers forum community.
- Keep the title short, descriptive, and in the form of a question.
- Provide enough details.
- Be clear and concise.
- Use correct spelling, punctuation, and capitalization.
- Add tags that represent the service or products you are asking about.
- This text editor supports [Markdown syntax](#) for things like headers, formatting, and lists.

[More tips »](#)

**B** *I* |      |     |   ?

Fill in the details...

Hint: You can notify a user about this post by typing @username.

Select a space for your question

Default

Tags

x qradar

Hint: Tags can contain more than one word; however, no space is allowed to separate multiple words.

Post your question

<https://ibm.biz/qradarforums> OR <https://developer.ibm.com/answers/questions/ask/?topics=qradar>

# Markdown Syntax and formatting questions

The dW Answers user interface has a standard text editor interface, however, the backend is driven using Markdown Syntax.

Users familiar with Reddit and other online forums might already be familiar with Markdown syntax, which is used to format posts. dW Answers also uses Markdown for formatting questions and responses.

Here are some examples:

For bulleted lists, use \* or + or -, but they must all be the same character in a column together:

- \* list item 1    • list item 1
- \* list item 2    • list item 2

For headings, use:

# for heading 1, titles for largest font

## for heading 2, secondary titles

### for heading 3

To bold text, use \*\* for example: **this is bold**

Ordered lists, just use numbers, for example:

- 1.
- 2.
- 3.

<https://ibm.biz/qradarforums> OR <https://developer.ibm.com/answers/questions/ask/?topics=qradar>

# Forum Migration Plans and what you need to know

In September, we will begin our migration. As questions come in to the existing forum, starting in mid-September users who ask questions in the old forums will have their answers completed in dW Answers and we will link to the answer in the new forum.

- **How does this affect me?**

For example, a users a question in the old forum we will not ignore it.

“How do I configure remote polling with stand-alone WinCollect?”

Our answer will be:

“Your answer is posted over in our new forums. See <link>. If you have follow-up questions, sign in using your IBM id to dW Answers to create an account as ask.

- **Will old content still be visible in the old forums?**

Yes, we plan to do a little forum cleanup for some old content, however, very few posts will be removed.

- **Can I still continue to use the old forums?**

You can ask questions in the old forums until mid-September. Any posts after today will include a footer reminding users about the new forum.

<https://ibm.biz/qradarforums> OR <https://developer.ibm.com/answers/questions/ask/?topics=qradar>

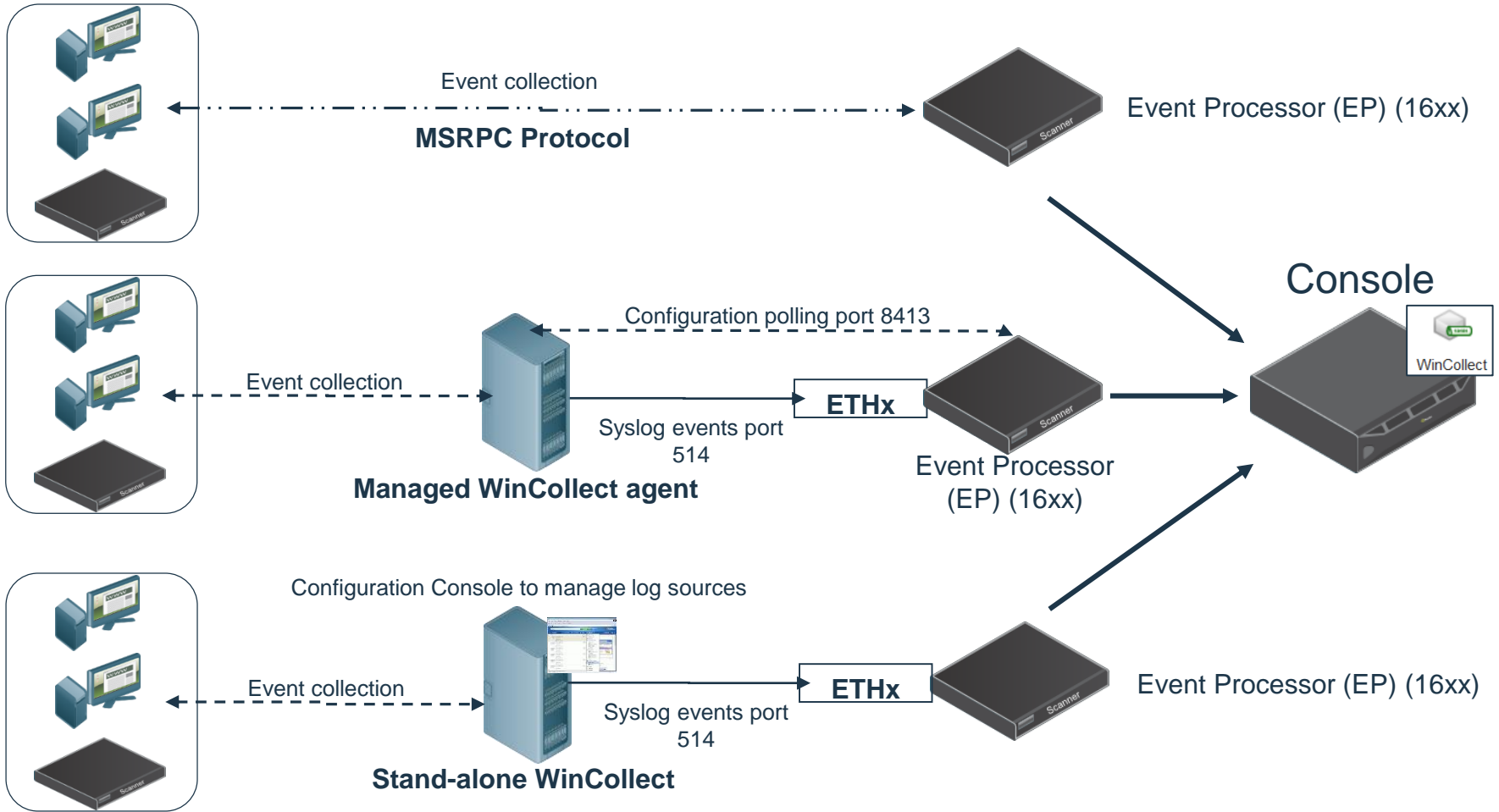




# WinCollect 7.2.4



# Overview of Windows Collection Options



Note: QRadar also supports Snare, Balabit IT Security, and other third-party software options.

# WinCollect Upgrade Paths

Minimum QRadar version:	Current Agent version:	Step 1	Step 2	Requirements
QRadar 7.0 MR5	7.0	No upgrade path. WinCollect 7.0 is the only version available for QRadar appliances at QRadar 7.0 MR5. An upgraded QRadar deployment is required.		
QRadar 7.1 MR2 Patch 1 or above	7.1.0	No upgrade path. WinCollect 7.1.0 requires an RPM and agent install. The Agent RPM on the Console must be installed before the administrator installs EXE files on the Windows host. See: <a href="http://www.ibm.com/support/docview.wss?uid=swg21698127">http://www.ibm.com/support/docview.wss?uid=swg21698127</a>		
	7.1.1	7.1.2	**7.2.2	** Ensure Port 443 & 8413 is open between the Console and the agent <b>BEFORE</b> you download and install the agent RPM on the Console from IBM Fix Central. Ensure that Enable Automatic Updates for the agent = true.
<ul style="list-style-type: none"> <li>▪ QRadar 7.1 MR2 Patch 1 or above</li> <li>▪ QRadar 7.2.0 or above</li> </ul>	7.1.2	**7.2.2-2	** Ensure Port 443 & 8413 is open between the Console and the agent <b>BEFORE</b> you download and install the agent RPM on the Console from IBM Fix Central. Ensure that Enable Automatic Updates for the agent = true. <b>ALWAYS</b> install the QRadar appliance software (SFS) before installing the EXEs on the Windows host. This prevents AES encryption key errors.	
	7.2.0 7.2.1 7.2.2 7.2.2-1	7.2.2-2	As WinCollect 7.2.0 is installed, port 8413 should be open. Ensure 'Enable Automatic Updates' for the agent = true. <b>ALWAYS</b> install the QRadar appliance software (SFS) before installing the EXEs on the Windows host. This prevents AES encryption key errors.	
<ul style="list-style-type: none"> <li>▪ QRadar 7.2.0 or above</li> </ul>	7.2.2-2	Upgrades to 7.2.3 or 7.2.4	A base required to upgrade to WinCollect 7.2.3 or 7.2.4 is WinCollect 7.2.2-2. If you are on an older version, you should consider upgrading to the latest WinCollect version before QRadar 7.3.	

## What's new in WinCollect 7.2.4?

- A new and improved installer will make installs easier and take the guesswork out of command-line installations.
- Stand Alone Mode installer supports log source autocreation
- New plug-in: DNS Debug is now available
- Updated plug-in: NetAPP DataONTAP for v8.3 (.EVTX file support)
- TLS Syslog support for TLS v1.0, TLS v1.1, and TLS v1.2
- New uninstaller cleans up files or can preserve configurations for reinstalls
- Simplified version numbers for filenames

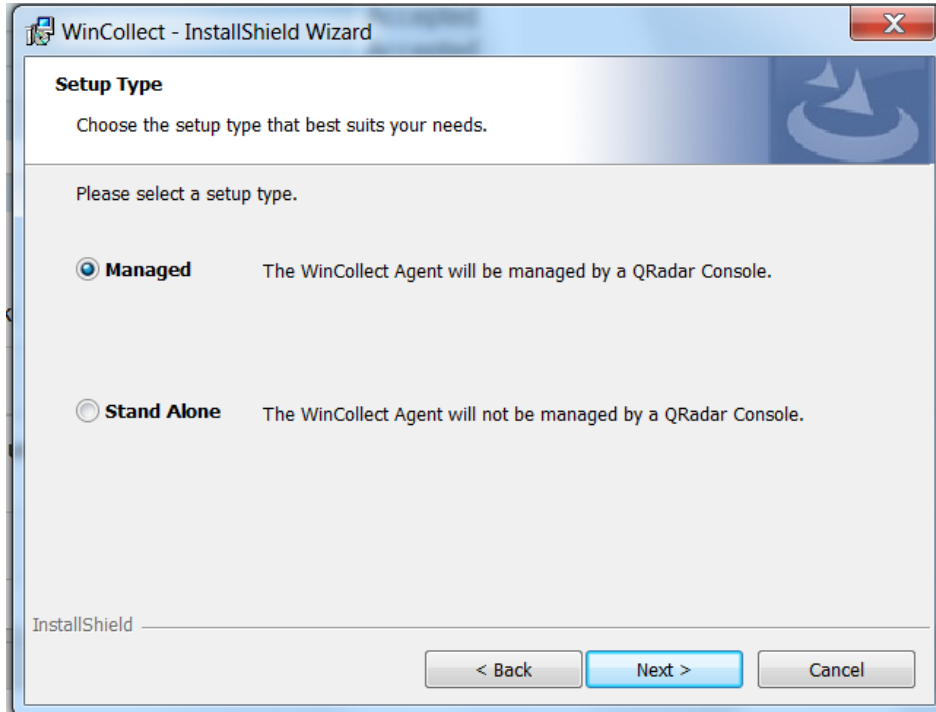


# WinCollect 7.2.4 Managed Installer



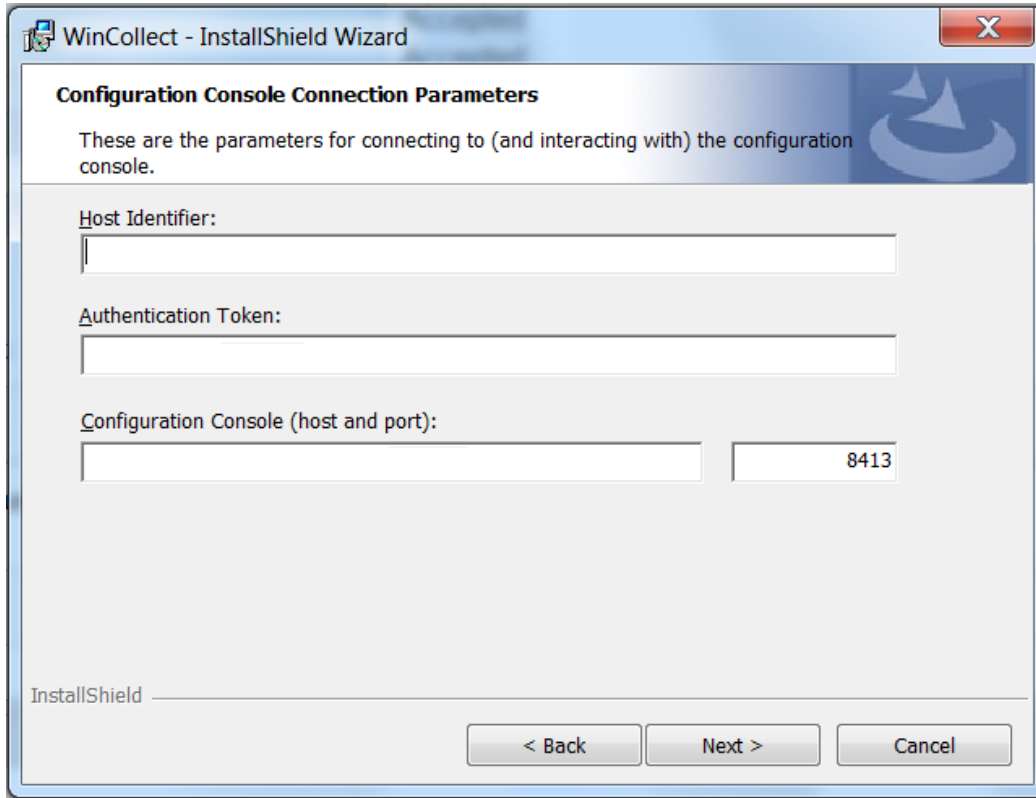
# WinCollect Installer Updates

The new installer now includes separate procedures for Managed vs Stand Alone mode.



# WinCollect Installer Updates

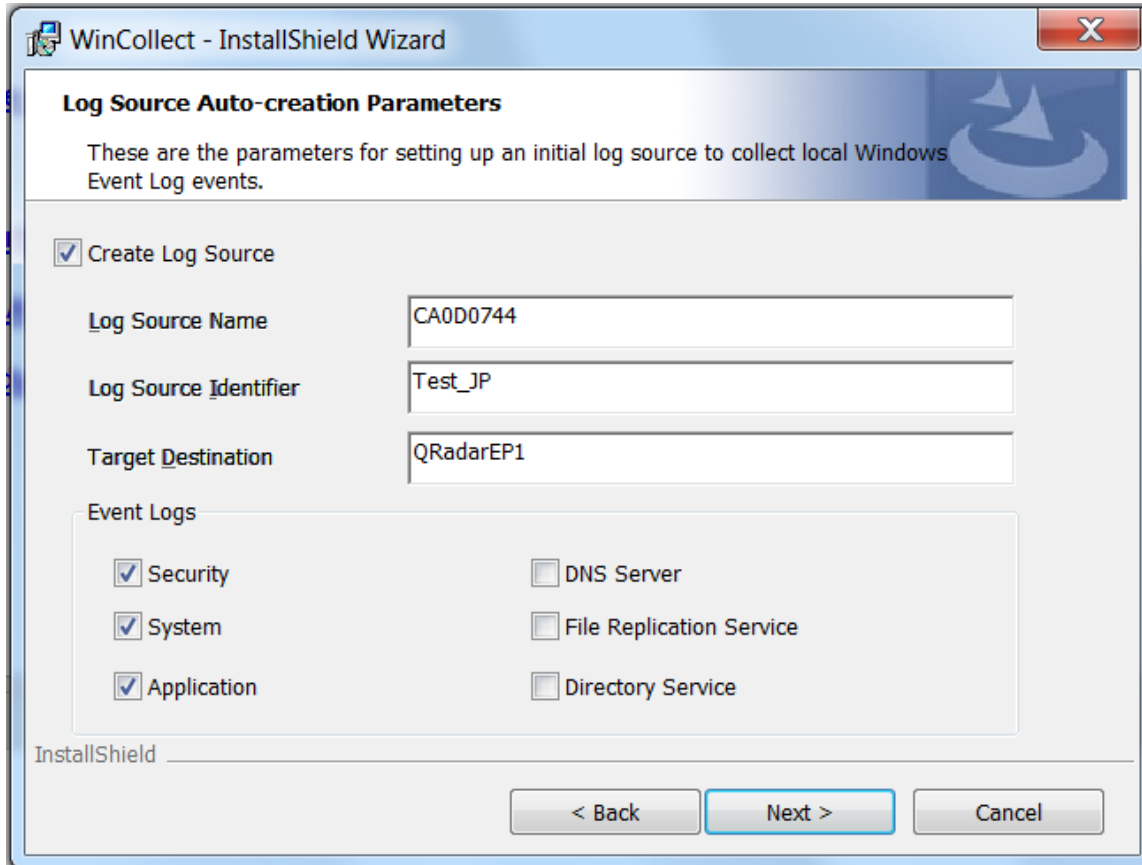
Managed installation configuration options in the updated WinCollect 7.2.4 installer.



The screenshot shows a Windows-style dialog box titled "WinCollect - InstallShield Wizard". The main heading is "Configuration Console Connection Parameters". Below the heading, there is a descriptive text: "These are the parameters for connecting to (and interacting with) the configuration console." The dialog contains three input fields: "Host Identifier:" (a single text box), "Authentication Token:" (a single text box), and "Configuration Console (host and port):" (two text boxes, with the second box containing the value "8413"). At the bottom, there are three buttons: "< Back", "Next >", and "Cancel". The "InstallShield" logo is visible in the bottom left corner of the dialog.

# WinCollect Installer Updates

Automatic log source configuration options. By default, the computer name is populated in the **Log Source Name** field.



The image shows a screenshot of the WinCollect - InstallShield Wizard dialog box. The title bar reads "WinCollect - InstallShield Wizard". The main heading is "Log Source Auto-creation Parameters". Below this, there is a descriptive text: "These are the parameters for setting up an initial log source to collect local Windows Event Log events." The dialog contains several input fields and checkboxes. The "Create Log Source" checkbox is checked. The "Log Source Name" field contains "CA0D0744". The "Log Source Identifier" field contains "Test\_IP". The "Target Destination" field contains "QRadarEP1". Under the "Event Logs" section, there are six checkboxes: "Security", "System", and "Application" are checked, while "DNS Server", "File Replication Service", and "Directory Service" are unchecked. At the bottom, there are three buttons: "< Back", "Next >", and "Cancel". The "Next >" button is highlighted with a blue border. The bottom left corner of the dialog shows "InstallShield".

**Log Source Auto-creation Parameters**

These are the parameters for setting up an initial log source to collect local Windows Event Log events.

Create Log Source

Log Source Name: CA0D0744

Log Source Identifier: Test\_IP

Target Destination: QRadarEP1

Event Logs

- Security
- System
- Application
- DNS Server
- File Replication Service
- Directory Service

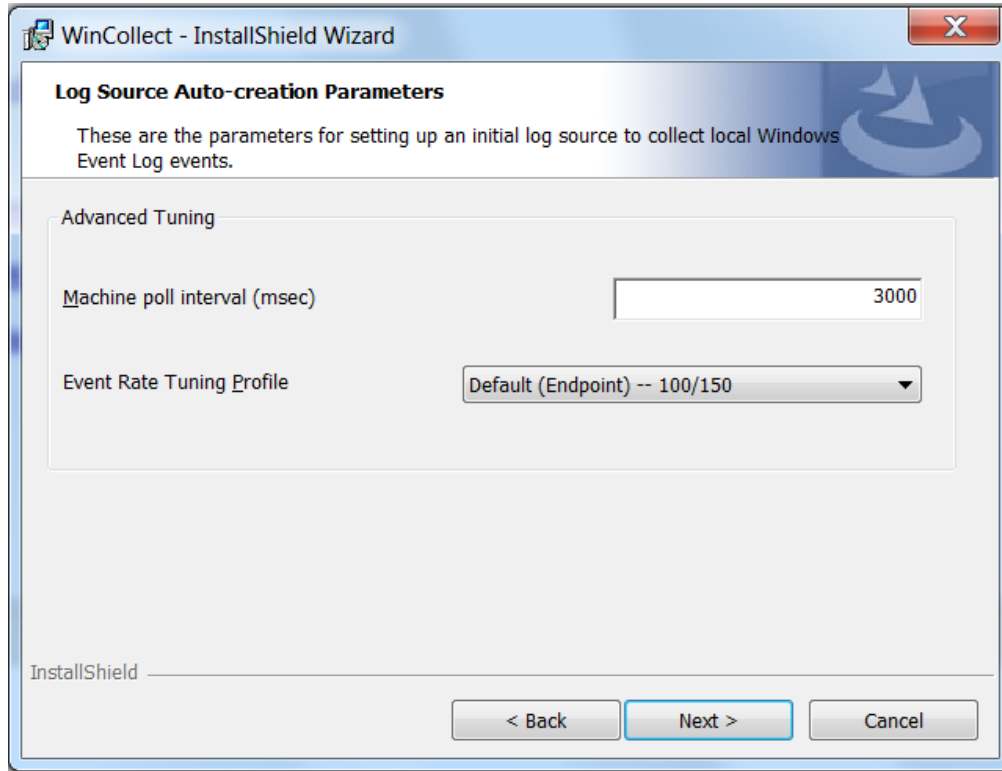
InstallShield

< Back   Next >   Cancel



# WinCollect Installer Updates

Log source tuning parameters.



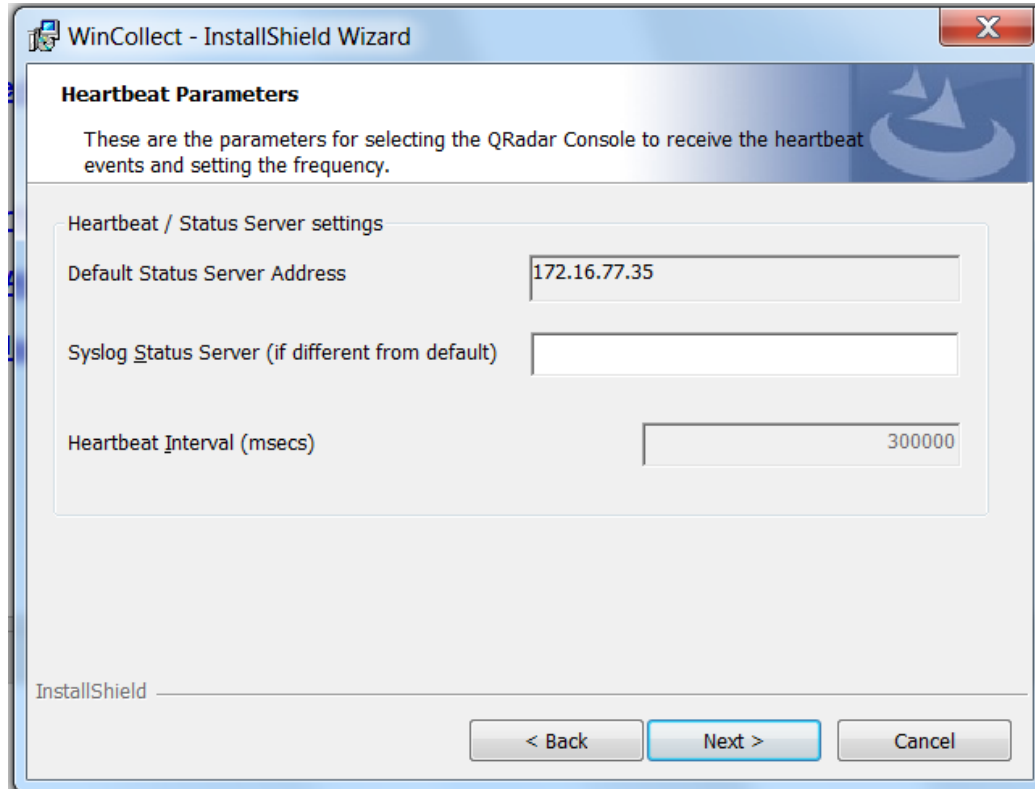
Event Rate Tuning Profile	Polling interval (ms)	Approximate EPS
Default (Endpoint) †	3000	40
Default (Endpoint)	2500	48
Default (Endpoint)	2000	60
Default (Endpoint)	1500	80
Default (Endpoint)	1250	96
Default (Endpoint)	1000	120
Default (Endpoint)	750	160
Default (Endpoint)	500	240
Default (Endpoint)	350	343
Typical Server	3000	200
Typical Server	2500	240
Typical Server	2000	300
Typical Server	1500	400
Typical Server	1250	480
Typical Server	1000	600
Typical Server	750	800
Typical Server	500	1200
Typical Server	350	1714
High Event Rate Server	3000	500
High Event Rate Server	2500	600
High Event Rate Server	2000	750
High Event Rate Server	1500	1000
High Event Rate Server	1250	1200
High Event Rate Server	1000	1500
High Event Rate Server	750	2000
High Event Rate Server*	600	2500
High Event Rate Server	500	3000
High Event Rate Server	450	3333
High Event Rate Server	350	4286
High Event Rate Server**	300	5000

† Indicates the default log source tuning parameters.

\* Indicates the maximum remote polling tuning option for a single agent

# WinCollect Installer Updates

New Heartbeat Parameters screen for configuring the Syslog Status Server and the interval at which the agent sends LEEF Syslog heartbeat messages. This is disabled for Managed mode installations.



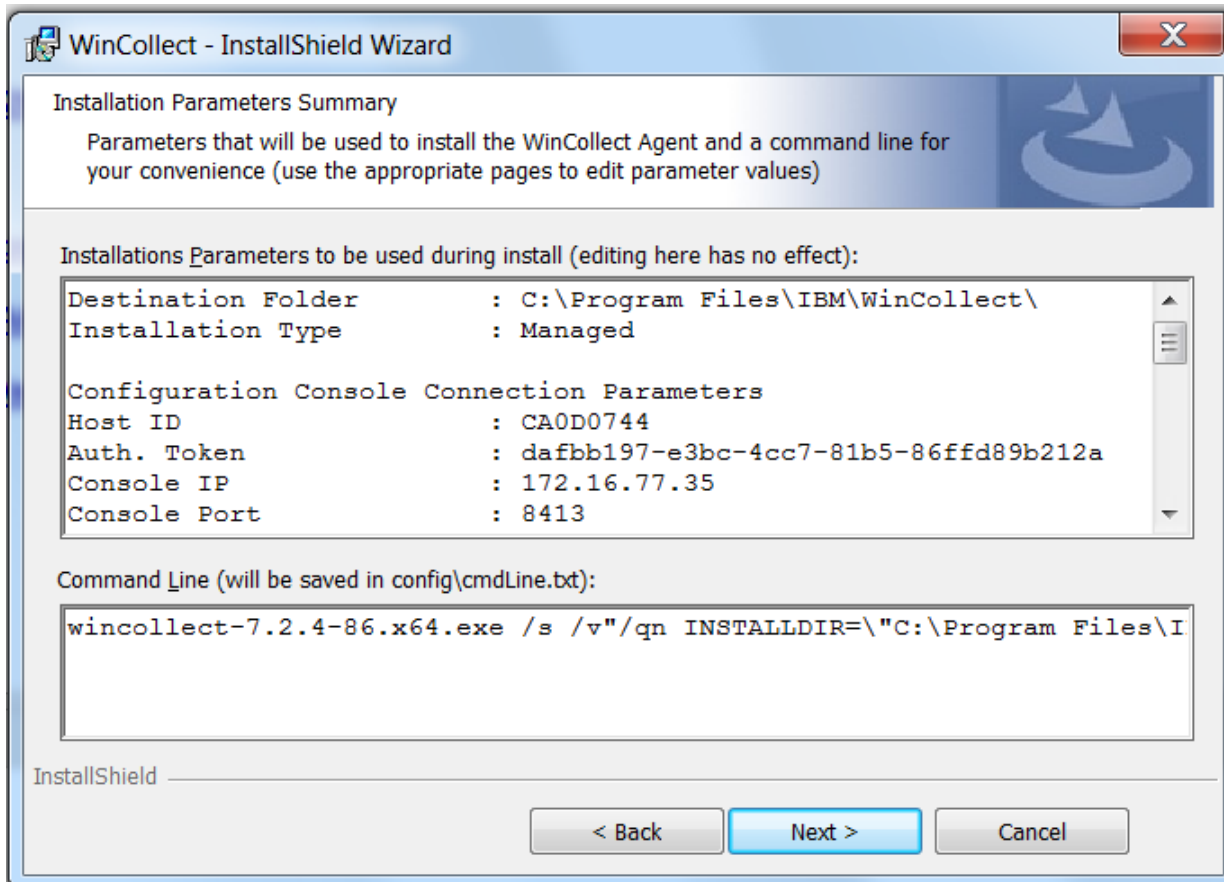
The screenshot shows a Windows-style dialog box titled "WinCollect - InstallShield Wizard". The main heading is "Heartbeat Parameters". Below the heading is a descriptive text: "These are the parameters for selecting the QRadar Console to receive the heartbeat events and setting the frequency." To the right of this text is a circular logo with a stylized 'S' and 'C'. The main area contains three input fields under the heading "Heartbeat / Status Server settings":

- "Default Status Server Address" with the value "172.16.77.35" entered.
- "Syslog Status Server (if different from default)" with an empty text box.
- "Heartbeat Interval (msecs)" with the value "300000" entered.

At the bottom of the dialog, there are three buttons: "< Back", "Next >" (which is highlighted with a blue border), and "Cancel". The "InstallShield" logo is visible in the bottom left corner.

# WinCollect Installer Updates

New summary screen allows you to review your parameters and provides you the command line installation text that can be modified and reused for other installs.



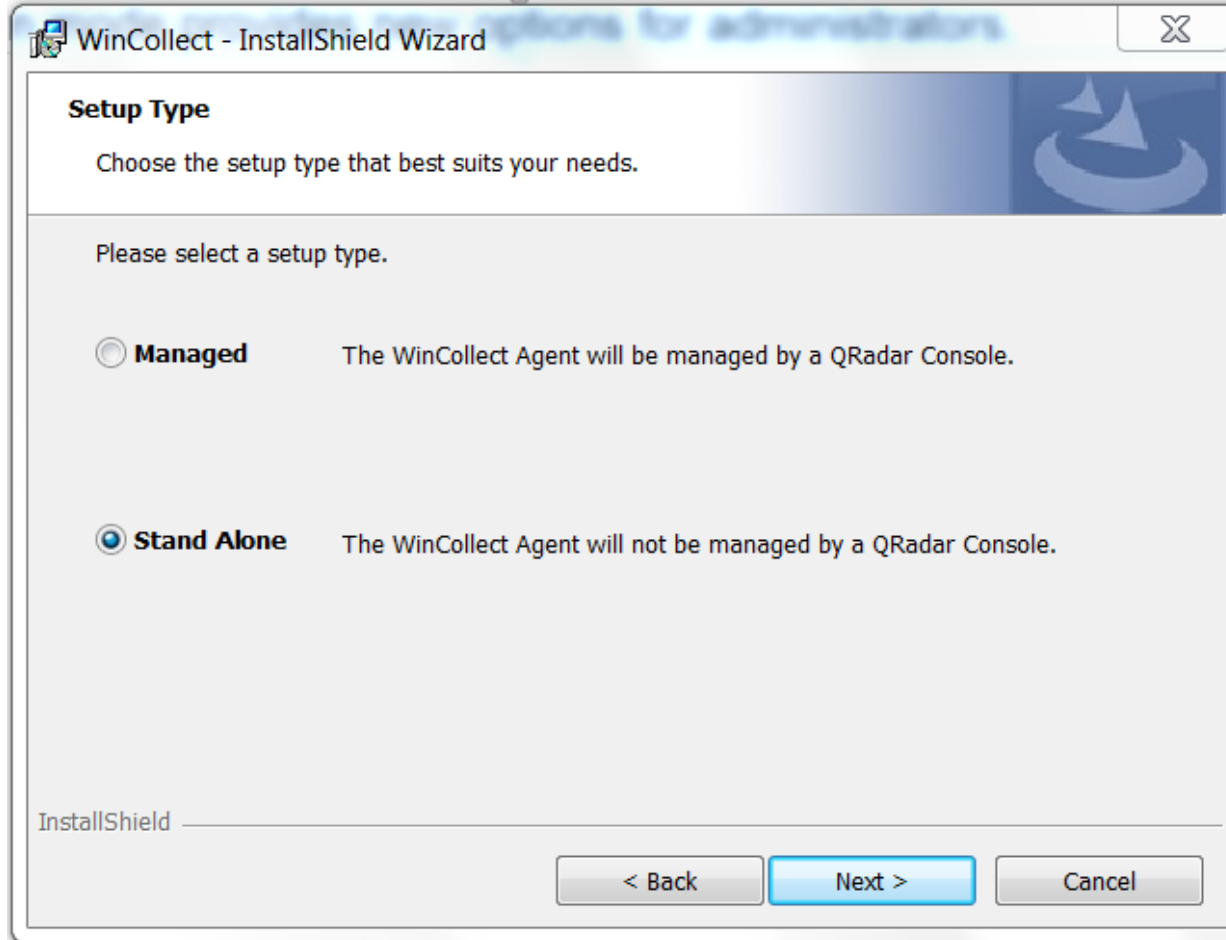


# WinCollect 7.2.4 Stand Alone Installer



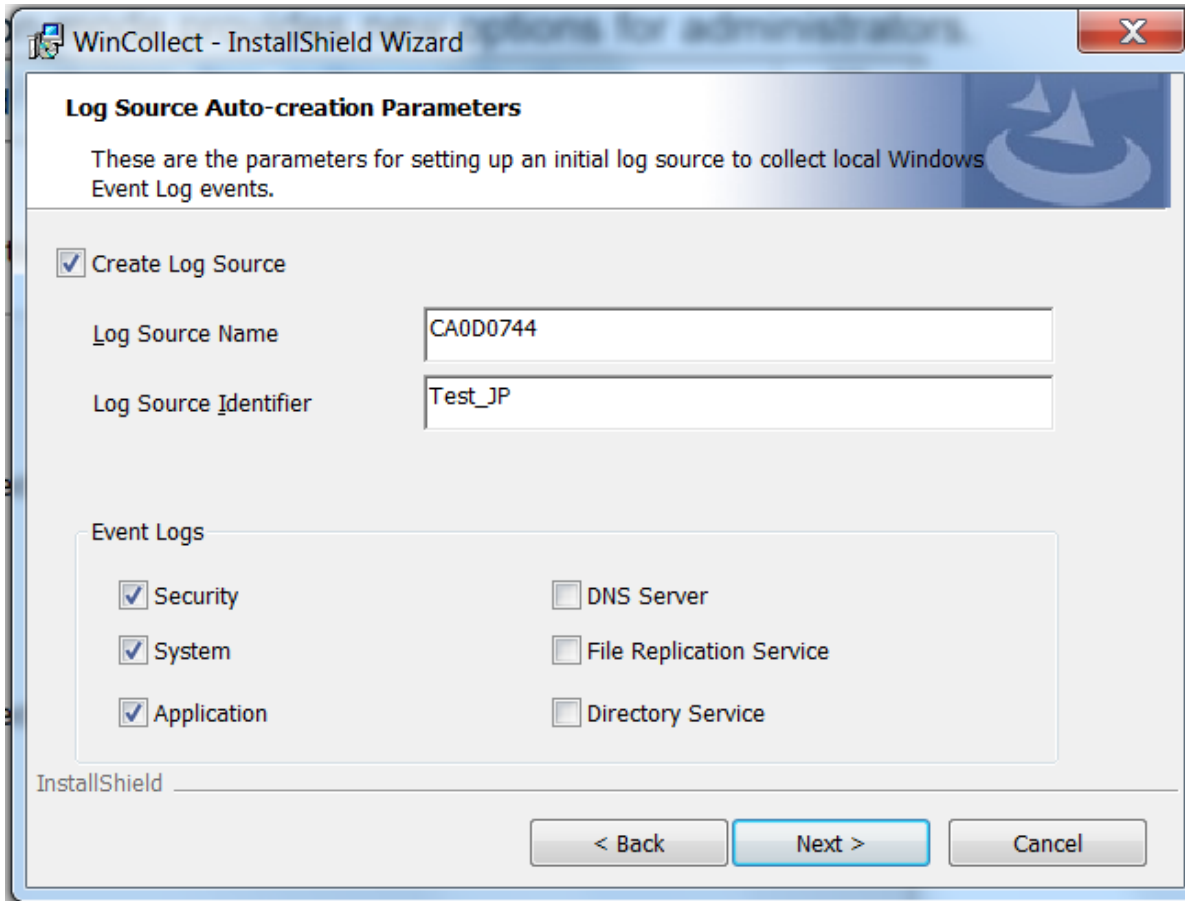
# WinCollect Installer – Stand Alone Mode

A new Stand Alone installation mode provides new options for administrators.



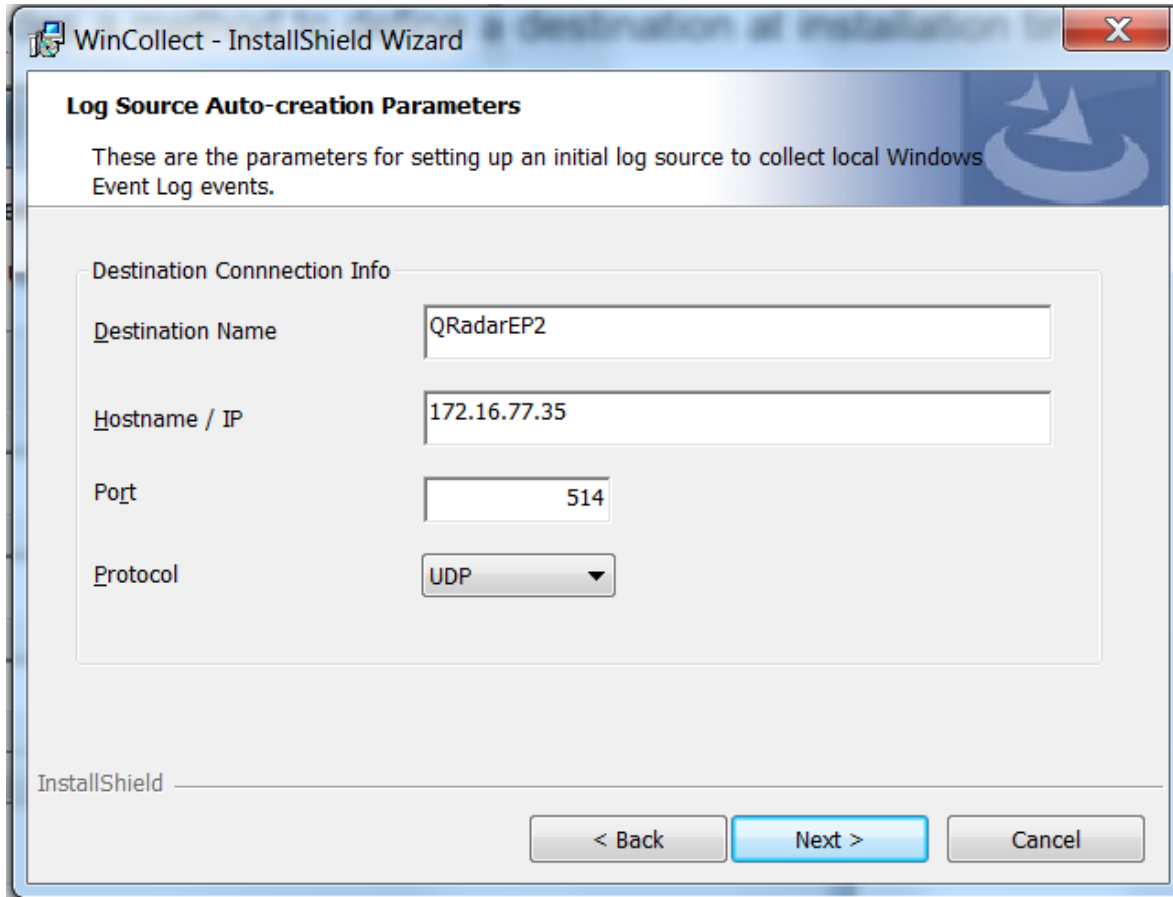
# WinCollect Installer – Stand Alone Mode

A new Stand Alone installation mode now allows a log source and destination to be specified.



# WinCollect Installer – Stand Alone Mode

The Stand Alone option provides a method to define a destination at installation time.



The image shows a screenshot of the WinCollect - InstallShield Wizard dialog box. The title bar reads "WinCollect - InstallShield Wizard" and includes a close button (X). The main content area is titled "Log Source Auto-creation Parameters" and contains the following text: "These are the parameters for setting up an initial log source to collect local Windows Event Log events." Below this text is a section titled "Destination Connection Info" which contains four input fields: "Destination Name" with the value "QRadarEP2", "Hostname / IP" with the value "172.16.77.35", "Port" with the value "514", and "Protocol" with a dropdown menu set to "UDP". At the bottom of the dialog box, there are three buttons: "< Back", "Next >" (highlighted in blue), and "Cancel". The "InstallShield" logo is visible in the bottom left corner of the dialog box.

**WinCollect - InstallShield Wizard**

**Log Source Auto-creation Parameters**

These are the parameters for setting up an initial log source to collect local Windows Event Log events.

**Destination Connection Info**

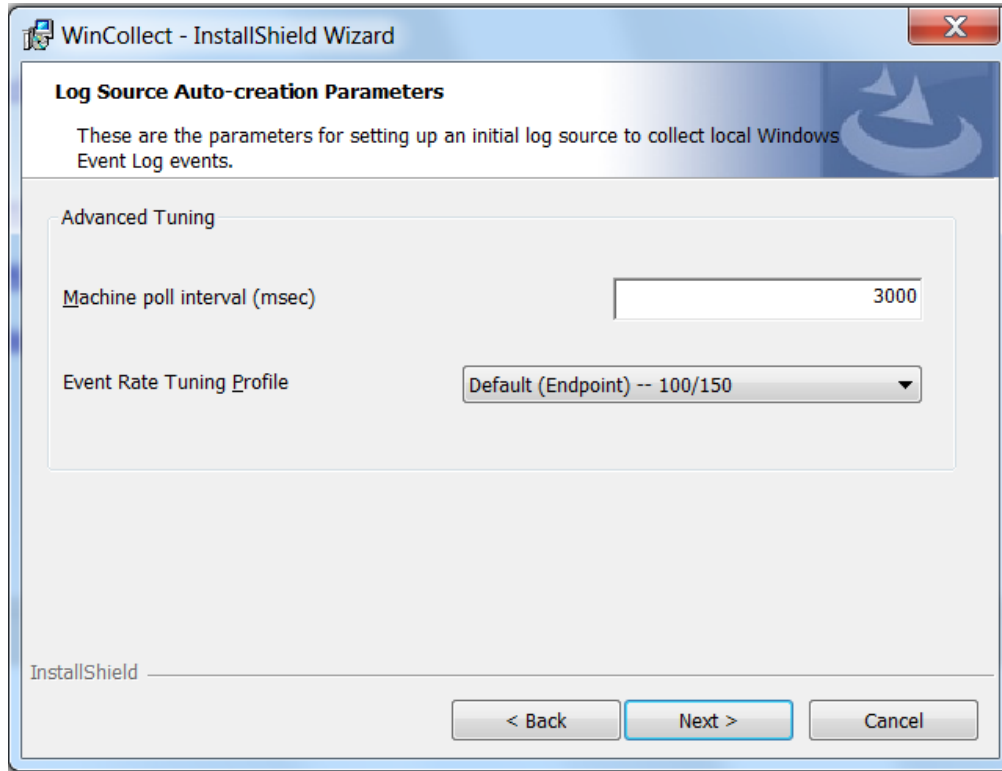
Destination Name	QRadarEP2
Hostname / IP	172.16.77.35
Port	514
Protocol	UDP

InstallShield

< Back   Next >   Cancel

# WinCollect Installer Updates

Log source tuning parameters.



Event Rate Tuning Profile	Polling interval (ms)	Approximate EPS
Default (Endpoint) †	3000	40
Default (Endpoint)	2500	48
Default (Endpoint)	2000	60
Default (Endpoint)	1500	80
Default (Endpoint)	1250	96
Default (Endpoint)	1000	120
Default (Endpoint)	750	160
Default (Endpoint)	500	240
Default (Endpoint)	350	343
Typical Server	3000	200
Typical Server	2500	240
Typical Server	2000	300
Typical Server	1500	400
Typical Server	1250	480
Typical Server	1000	600
Typical Server	750	800
Typical Server	500	1200
Typical Server	350	1714
High Event Rate Server	3000	500
High Event Rate Server	2500	600
High Event Rate Server	2000	750
High Event Rate Server	1500	1000
High Event Rate Server	1250	1200
High Event Rate Server	1000	1500
High Event Rate Server	750	2000
High Event Rate Server*	600	2500
High Event Rate Server	500	3000
High Event Rate Server	450	3333
High Event Rate Server	350	4286
High Event Rate Server**	300	5000

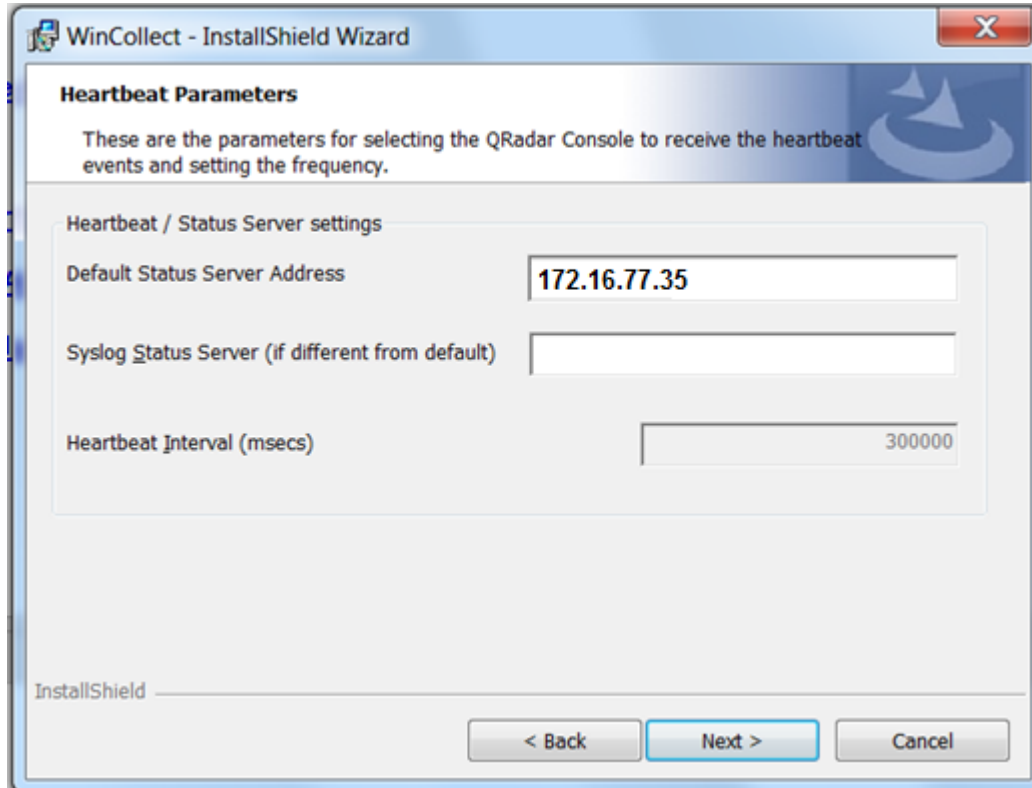
† Indicates the default log source tuning parameters.

\* Indicates the maximum remote polling tuning option for a single agent



# WinCollect Installer Updates

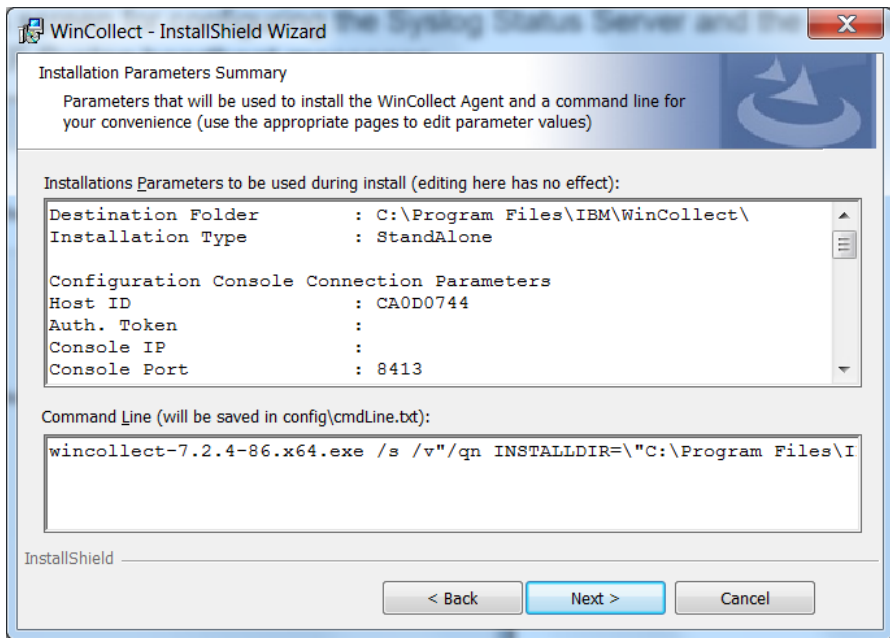
New Heartbeat Parameters screen for configuring the Syslog Status Server and the interval at which the agent sends LEEF Syslog heartbeat messages.



```
<13>Nov 30 11:01:46 192.168.XXX.XX1 LEEF:1.0|IBM|WinCollect|7.2|2|src=192.168.XXX.XX1  
dst=192.168.XXX.XX2 sev=3 log=Code.SSLConfigServerConnection msg=ApplicationHeartbeat
```

# WinCollect Installer Updates

New Heartbeat Parameters screen for configuring the Syslog Status Server and the interval at which the agent sends LEEF Syslog heartbeat messages.



```
wincollect-7.2.4-86.x64.exe /s /v"/qn INSTALLDIR="C:\Program Files\IBMWinCollect" LOG_SOURCE_AUTO_CREATION_ENABLED=True  
LOG_SOURCE_AUTO_CREATION_PARAMETERS=""Component1.AgentDevice=DeviceWindowsLog&Component1.Action=create&Component1.  
LogSourceName=CA0D0744&Component1.LogSourceIdentifier=Test_JP&Component1.Dest.Name=QRadarEP2&Component1.Dest.Hostname=17  
2.16.77.35&Component1.Dest.Port=514&Component1.Dest.Protocol=UDP&Component1.Log.Security=true&Component1.Log.System=true&Comp  
onent1.Log.Application=true&Component1.Log.DNS+Server=false&Component1.Log.File+Replication+Service=false&Component1.Log.Directory+S  
ervice=false&Component1.RemoteMachinePollInterval=3000&Component1.EventRateTuningProfile=Default+(Endpoint)&Component1.MinLogsToP  
rocessPerPass=100&Component1.MaxLogsToProcessPerPass=150""
```



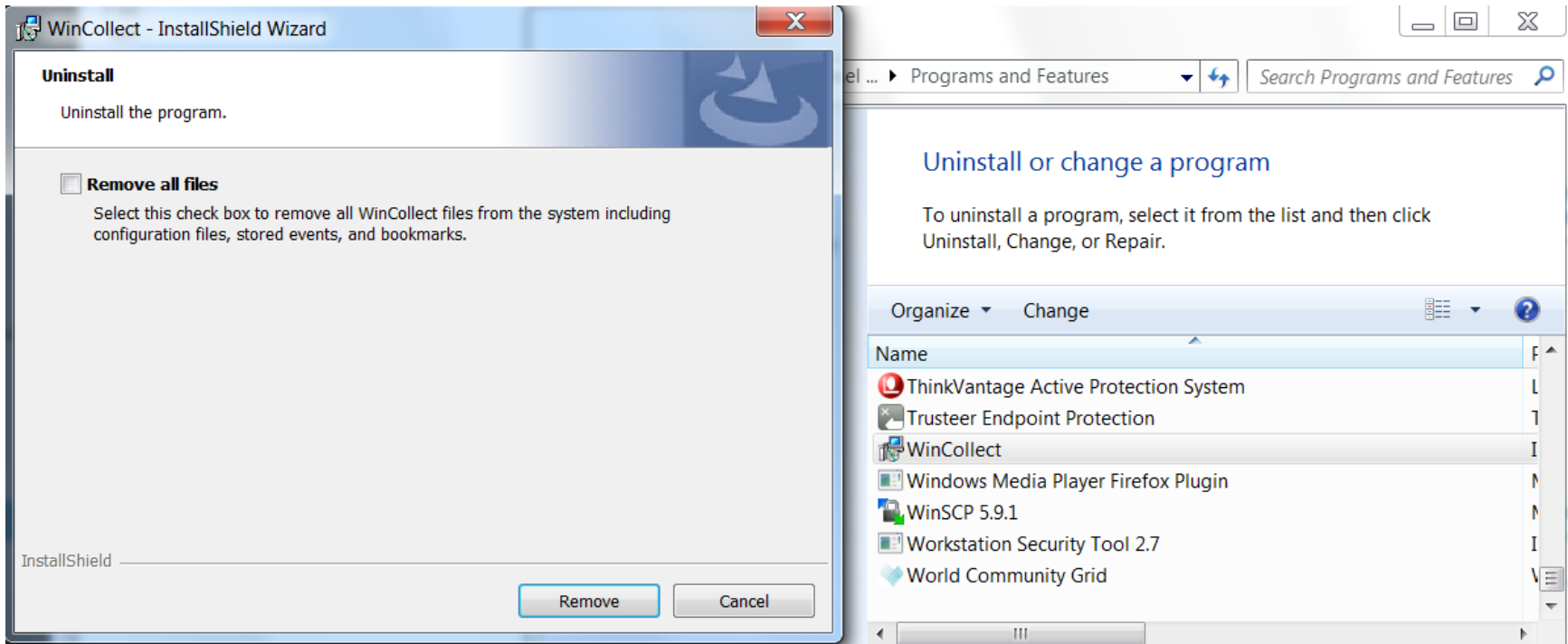
# WinCollect 7.2.4 Uninstaller



# WinCollect Installer Updates

New summary screen allows you to review your parameters and provides you the command line installation text that can be modified and reused for other installs.

Removing files cleans up all data that is in %ProgramData%\WinCollect






# WinCollect 7.2.4 TLS Syslog Update



# TLS Syslog Update

Administrators might notice that the `install_config.txt` file contains new parameters to control the minimum and maximum TLS Protocol version that WinCollect is allowed to use.

```
ApplicationIdentifier=CA0D0744  
ConfigurationServer=  
ConfigurationServerPort=8413  
ConfigurationServerMinSSLProtocol=TLSv1  
ConfigurationServerMaxSSLProtocol=TLSv1.2  
StatusServer=172.16.77.35:514  
ApplicationToken=  
BuildNumber=86
```



# WinCollect 7.2.4 Custom LEEF Heartbeat Messages



# WinCollect Custom LEEF Heartbeat Messages

Another change that is new is to add a unique payload value to a WinCollect heartbeat LEEF status messages. These heartbeat messages have been improved to contain both the operating system (os=) with build information and the source computer name (src=) to more easily identify the computer sending a heartbeat message.

To create a custom heartbeat message:

1. Log in to a Windows host with WinCollect 7.2.4 installed.
2. Navigate to *C:\Program Files\IBM\WinCollect\config*
3. Create a text file named **heartbeat\_custom.props**.
4. Add unique heartbeat values as name value pairs, one pair per line of the properties file.

Example:

```
function=domaincontroller  
region=US  
building=2
```

```
<13>Jul 22 15:02:48 CA0D0744 LEEF:1.0|IBM|WinCollect|7.2.4.86|2| src=SERVER-03  
os=Windows 10(Build 10240 64-bit)dst= sev=3 log=Code.SSLConfigServerConnection  
function=domaincontroller region=us building=2 msg=ApplicationHeartbeat
```



# WinCollect Custom LEEF Heartbeat Messages


## Restrictions:


- You cannot use reserved LEEF keys from the predefined event values list:
  - srcPort
  - src
  - usrName
  - srcMAC
  - dst
  - identSrc
  - vSrc
  - accountName
  - srcBytes
  - Etc... See the LEEF Guide for the complete list: <http://ibm.biz/leefv2guide>
- Special characters are not allowed, such as = | [ ] { } < > / \ ' "
- The property file cannot exceed 10KB.
- Custom entries must be alpha-numeric values and not contain spaces.  
Example: `function=domain controller` is bad  
`function=domaincontroller` is acceptable
- Multiple white spaces are reduced to a single space.



# THANK YOU

## FOLLOW US ON:

 <https://www.facebook.com/IBM-Security-Support-221766828033861/>

 QRadar Forums: <https://ibm.biz/BdR2kC>

 [youtube/user/ibmsecuritysupport](https://www.youtube.com/user/ibmsecuritysupport)

 [@askibmsecurity](https://twitter.com/askibmsecurity)

 [securityintelligence.com](https://securityintelligence.com)

 [xforce.ibmcloud.com](https://xforce.ibmcloud.com)

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.