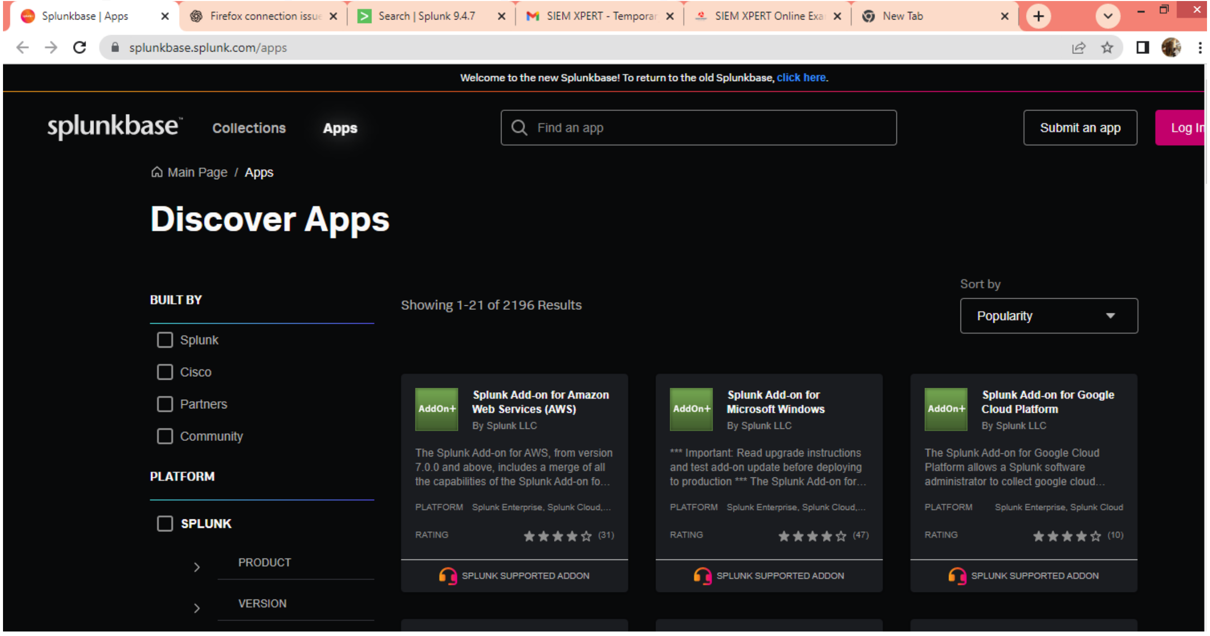
Adding Windows_ADD_On_SearchHead

Step 1: Download the Add-on

1. Go to **Splunkbase** https://splunkbase.splunk.com/apps



Welcome to the new Splunkbase! To return to the old Splunkbase, click here.

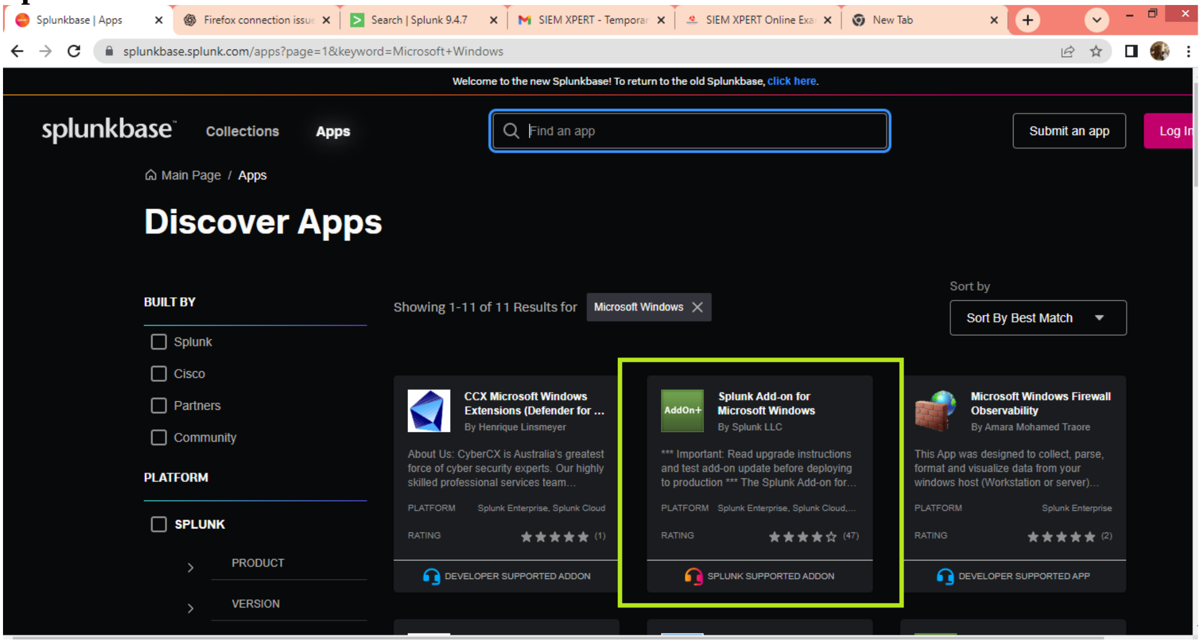
Showing 1-21 of 2196 Results

Splunk Add-on for Amazon Web Services (AWS)
By Splunk LLC
The Splunk Add-on for AWS, from version 7.0.0 and above, includes a merge of all the capabilities of the Splunk Add-on fo...
PLATFORM Splunk Enterprise, Splunk Cloud,...
RATING ★★★★★ (31)

Splunk Add-on for Microsoft Windows
By Splunk LLC
*** Important: Read upgrade instructions and test add-on update before deploying to production *** The Splunk Add-on for...
PLATFORM Splunk Enterprise, Splunk Cloud,...
RATING ★★★★☆ (47)

Splunk Add-on for Google Cloud Platform
By Splunk LLC
The Splunk Add-on for Google Cloud Platform allows a Splunk software administrator to collect google cloud...
PLATFORM Splunk Enterprise, Splunk Cloud
RATING ★★★★☆ (10)

2.
3. Search for:
Splunk Add-on for Microsoft Windows



Welcome to the new Splunkbase! To return to the old Splunkbase, click here.

Showing 1-11 of 11 Results for Microsoft Windows

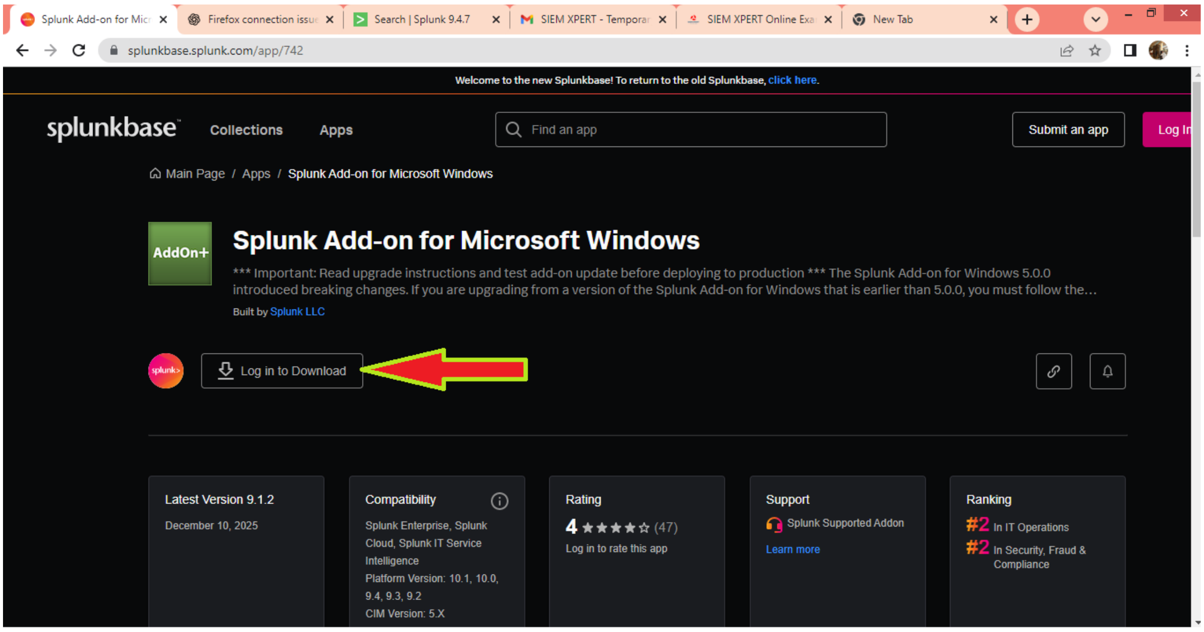
CCX Microsoft Windows Extensions (Defender for ...
By Henrique Linsmeyer
About Us: CyberCX is Australia's greatest force of cyber security experts. Our highly skilled professional services team...
PLATFORM Splunk Enterprise, Splunk Cloud
RATING ★★★★★ (1)
DEVELOPER SUPPORTED ADDON

Splunk Add-on for Microsoft Windows
By Splunk LLC
*** Important: Read upgrade instructions and test add-on update before deploying to production *** The Splunk Add-on for...
PLATFORM Splunk Enterprise, Splunk Cloud,...
RATING ★★★★☆ (47)
SPLUNK SUPPORTED ADDON

Microsoft Windows Firewall Observability
By Amara Mohamed Traore
This App was designed to collect, parse, format and visualize data from your windows host (Workstation or server)...
PLATFORM Splunk Enterprise
RATING ★★★★★ (2)
DEVELOPER SUPPORTED APP

4.

5.



Welcome to the new Splunkbase! To return to the old Splunkbase, click here.

Main Page / Apps / Splunk Add-on for Microsoft Windows

Splunk Add-on for Microsoft Windows

*** Important: Read upgrade instructions and test add-on update before deploying to production *** The Splunk Add-on for Windows 5.0.0 introduced breaking changes. If you are upgrading from a version of the Splunk Add-on for Windows that is earlier than 5.0.0, you must follow the...

Built by Splunk LLC

Latest Version 9.1.2
December 10, 2025

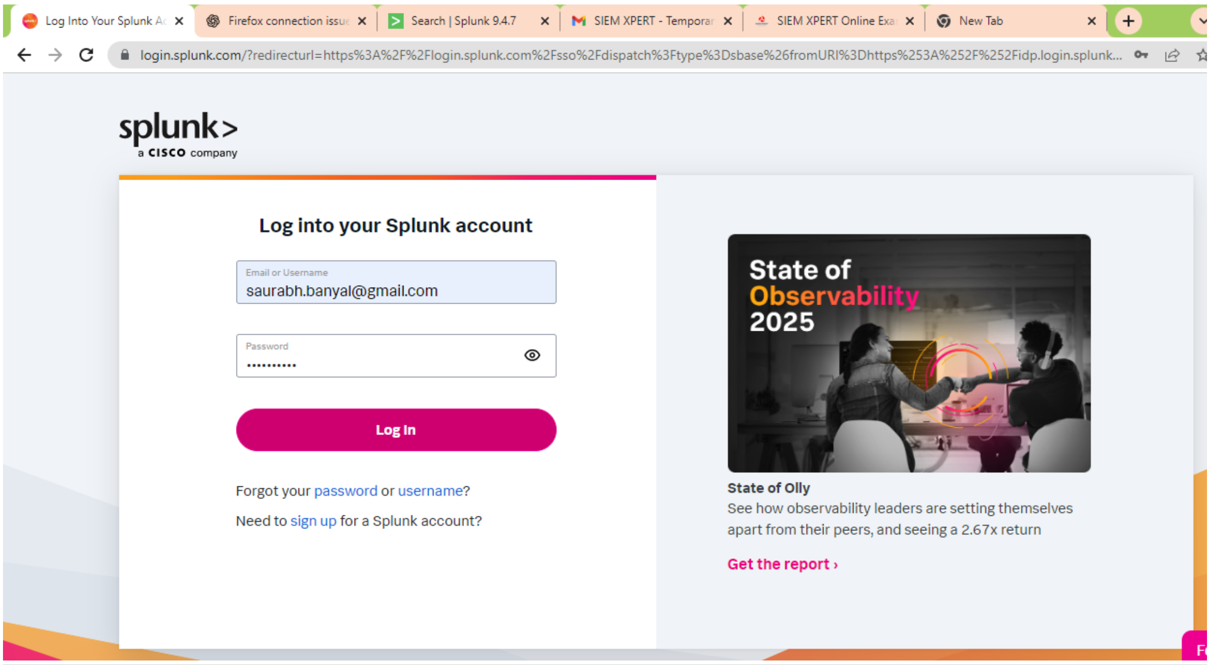
Compatibility
Splunk Enterprise, Splunk Cloud, Splunk IT Service Intelligence
Platform Version: 10.1, 10.0, 9.4, 9.3, 9.2
CIM Version: 5.X

Rating
4 ★★★★☆ (47)
Log in to rate this app

Support
Splunk Supported Addon
Learn more

Ranking
#2 In IT Operations
#2 In Security, Fraud & Compliance

6.


Log Into Your Splunk A
Firefox connection issu
Search | Splunk 9.4.7
SIEM XPERT - Tempora
SIEM XPERT Online Exa
New Tab
login.splunk.com/?redirecturl=https%3A%2F%2Flogin.splunk.com%2Fsso%2Fdispatch%3Ftype%3Dsbase%26fromURI%3Dhttps%253A%252F%252Fidp.login.splunk...
splunk>
a CISCO company

Log into your Splunk account

Email or Username
saurabh.banyal@gmail.com

Password
....

Forgot your password or username?

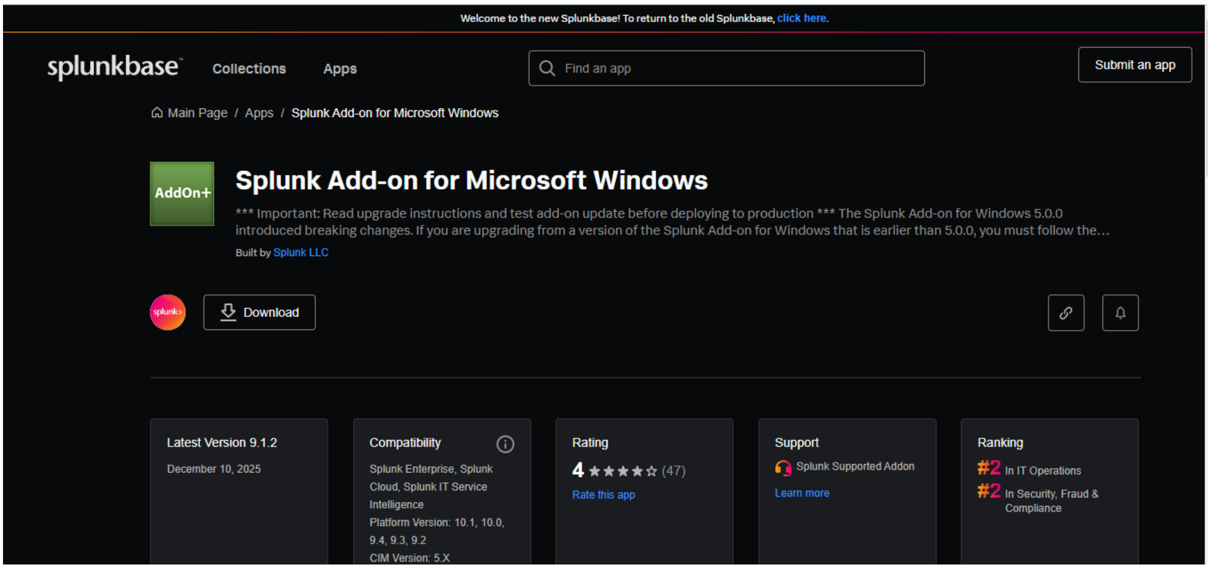
Need to sign up for a Splunk account?

State of Observability 2025

State of Olly

See how observability leaders are setting themselves apart from their peers, and seeing a 2.67x return

7.


Welcome to the new Splunkbase! To return to the old Splunkbase, click here.

Main Page / Apps / Splunk Add-on for Microsoft Windows

Splunk Add-on for Microsoft Windows

*** Important: Read upgrade instructions and test add-on update before deploying to production *** The Splunk Add-on for Windows 5.0.0 introduced breaking changes. If you are upgrading from a version of the Splunk Add-on for Windows that is earlier than 5.0.0, you must follow the...

Built by Splunk LLC

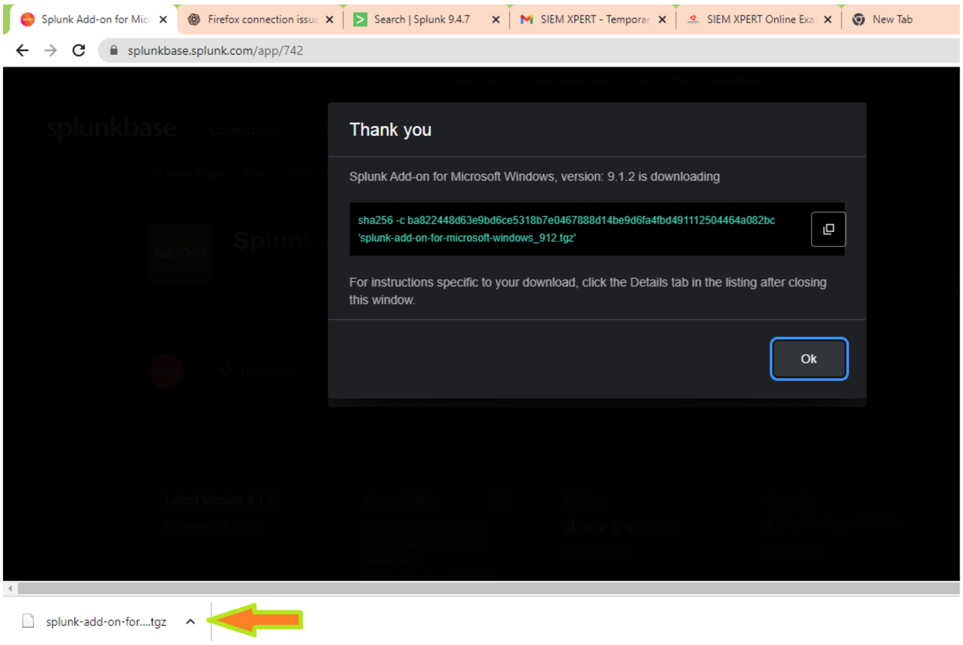
Latest Version 9.1.2
December 10, 2025

Compatibility
Splunk Enterprise, Splunk Cloud, Splunk IT Service Intelligence
Platform Version: 10.1, 10.0, 9.4, 9.3, 9.2
CIM Version: 5.X

Rating
4 ★★★★☆ (47)
Rate this app

Support
Splunk Supported Addon
Learn more

Ranking
#2 In IT Operations
#2 In Security, Fraud & Compliance



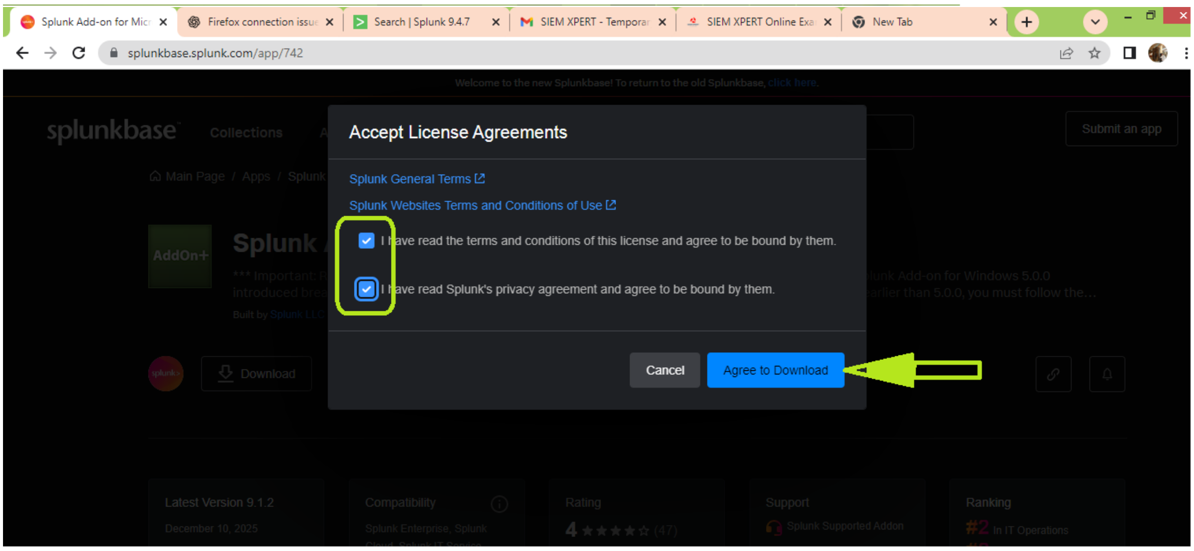
Thank you

Splunk Add-on for Microsoft Windows, version: 9.1.2 is downloading

```
sha256 -c ba822448d63e9bd6ce5318b7e0467888d14be9d6fa4fbd491112504464a082bc
'splunk-add-on-for-microsoft-windows_912.tgz'
```

For instructions specific to your download, click the Details tab in the listing after closing this window.

8.



Accept License Agreements

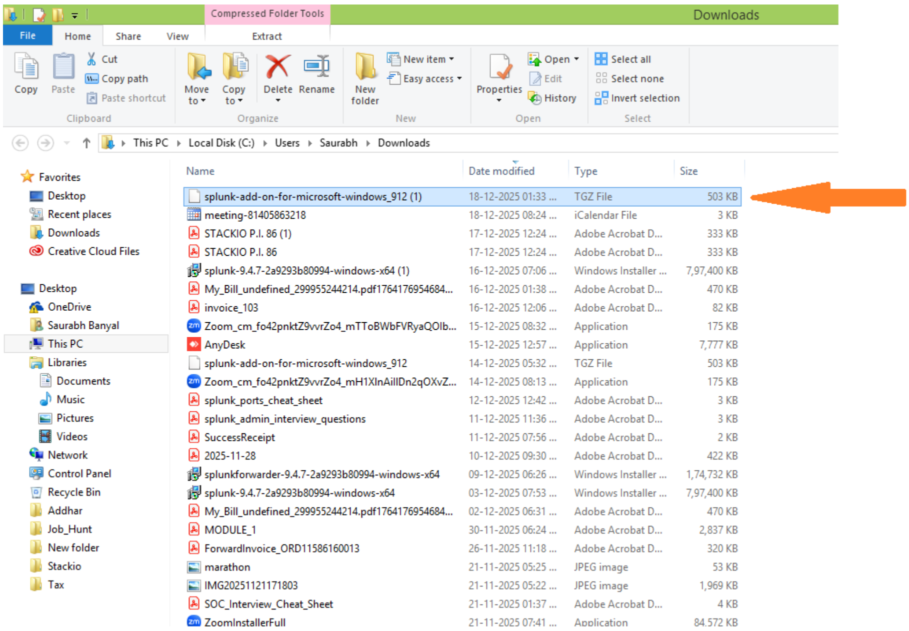
Splunk General Terms

Splunk Websites Terms and Conditions of Use

☑ I have read the terms and conditions of this license and agree to be bound by them.

☑ I have read Splunk's privacy agreement and agree to be bound by them.

9. Download the `.spl` file



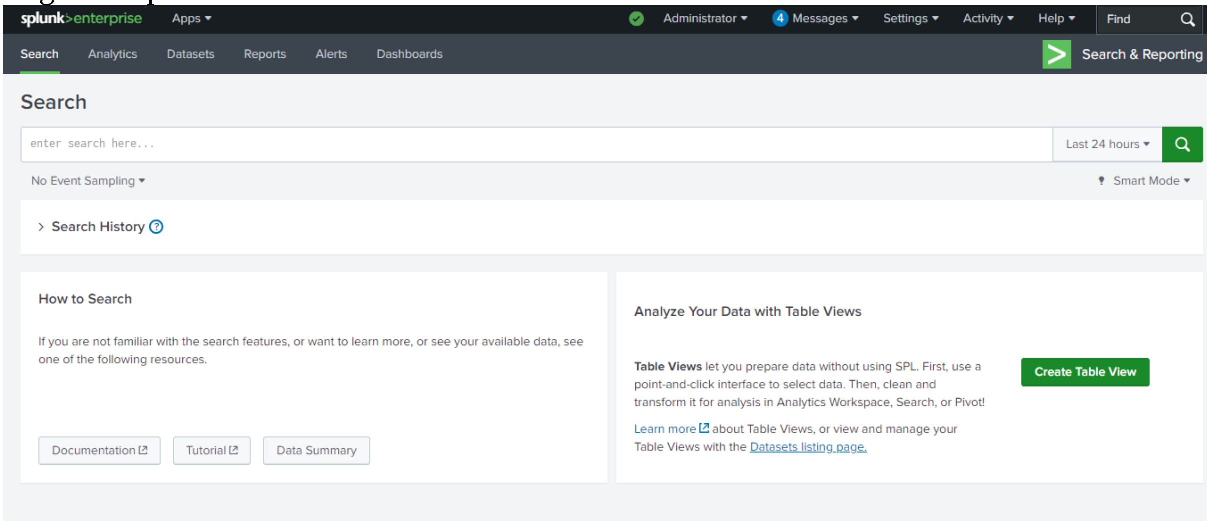
Name	Date modified	Type	Size
splunk-add-on-for-microsoft-windows_912 (1)	18-12-2025 01:33 ...	TGZ File	503 KB
meeting-81405863218	18-12-2025 08:24 ...	iCalendar File	3 KB
STACKIO P.I. 86 (1)	17-12-2025 12:24 ...	Adobe Acrobat D...	333 KB
STACKIO P.I. 86	17-12-2025 12:24 ...	Adobe Acrobat D...	333 KB
splunk-9.4.7-2a9293b80994-windows-x64 (1)	16-12-2025 07:06 ...	Windows Installer ...	7,97,400 KB
My_Bill_undefined_299955244214.pdf1764176954684...	16-12-2025 01:38 ...	Adobe Acrobat D...	470 KB
invoice_103	16-12-2025 12:06 ...	Adobe Acrobat D...	82 KB
Zoom_cm_fo42pnktZ9vvrZo4_mTToBWbFVRyaQOlb...	15-12-2025 08:32 ...	Application	175 KB
AnyDesk	15-12-2025 12:57 ...	Application	7,777 KB
splunk-add-on-for-microsoft-windows_912	14-12-2025 05:32 ...	TGZ File	503 KB
Zoom_cm_fo42pnktZ9vvrZo4_mH1XlnAillDn2qOXvZ...	14-12-2025 08:13 ...	Application	175 KB
splunk_ports_cheat_sheet	12-12-2025 12:42 ...	Adobe Acrobat D...	3 KB
splunk_admin_interview_questions	11-12-2025 11:36 ...	Adobe Acrobat D...	3 KB
SuccessReceipt	11-12-2025 07:56 ...	Adobe Acrobat D...	2 KB
2025-11-28	10-12-2025 09:30 ...	Adobe Acrobat D...	422 KB
splunkforwarder-9.4.7-2a9293b80994-windows-x64	09-12-2025 06:26 ...	Windows Installer ...	1,74,732 KB
splunk-9.4.7-2a9293b80994-windows-x64	03-12-2025 07:53 ...	Windows Installer ...	7,97,400 KB
My_Bill_undefined_299955244214.pdf1764176954684...	02-12-2025 06:31 ...	Adobe Acrobat D...	470 KB
MODULE_1	30-11-2025 06:24 ...	Adobe Acrobat D...	2,837 KB
ForwardInvoice_ORD11586160013	26-11-2025 11:18 ...	Adobe Acrobat D...	320 KB
marathon	21-11-2025 05:25 ...	JPEG image	53 KB
IMG20251121171803	21-11-2025 05:22 ...	JPEG image	1,969 KB
SOC_Interview_Cheat_Sheet	21-11-2025 01:37 ...	Adobe Acrobat D...	4 KB
ZoomInstallerFull	21-11-2025 07:41 ...	Application	84,572 KB

10.

◆ Step 2: Install on the Search Head

Using Splunk Web (Recommended)

1. Log in to Splunk Web on the **Search Head**



How to Search

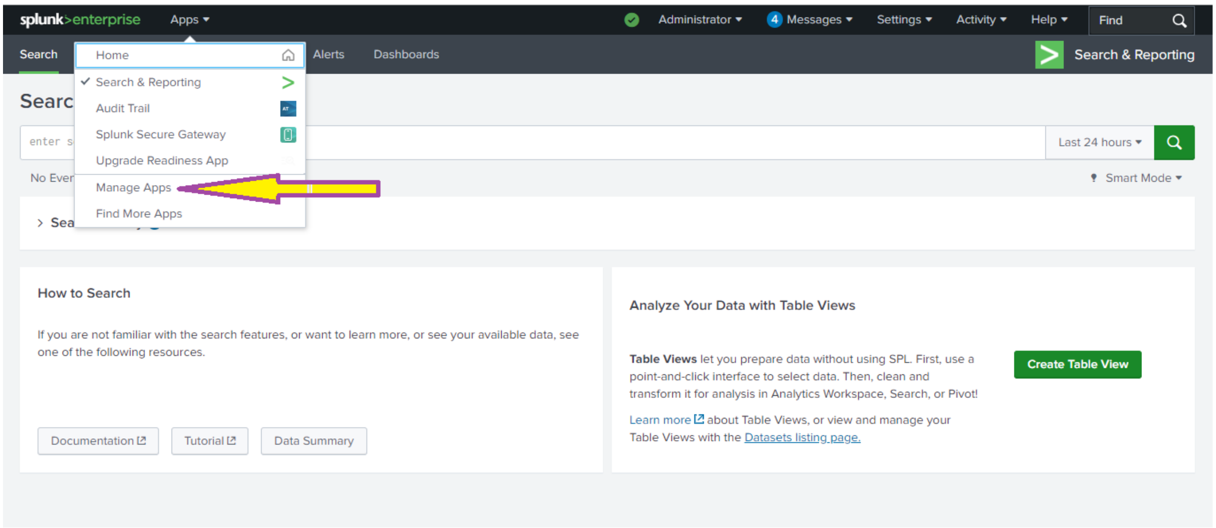
If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.

Analyze Your Data with Table Views

Table Views let you prepare data without using SPL. First, use a point-and-click interface to select data. Then, clean and transform it for analysis in Analytics Workspace, Search, or Pivot!

Learn more about Table Views, or view and manage your Table Views with the Datasets listing page.

2.
3. Go to:
4. `Apps → Manage Apps → Install app from file`



How to Search

If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.

Documentation | Tutorial | Data Summary

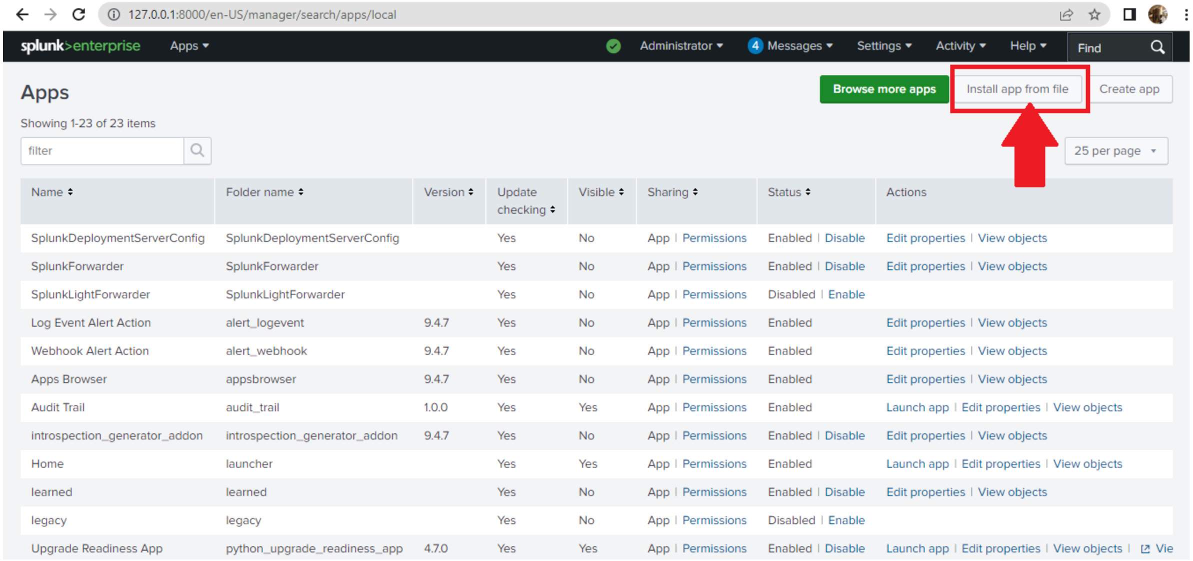
Analyze Your Data with Table Views

Table Views let you prepare data without using SPL. First, use a point-and-click interface to select data. Then, clean and transform it for analysis in Analytics Workspace, Search, or Pivot!

Create Table View

Learn more about Table Views, or view and manage your Table Views with the Datasets listing page.

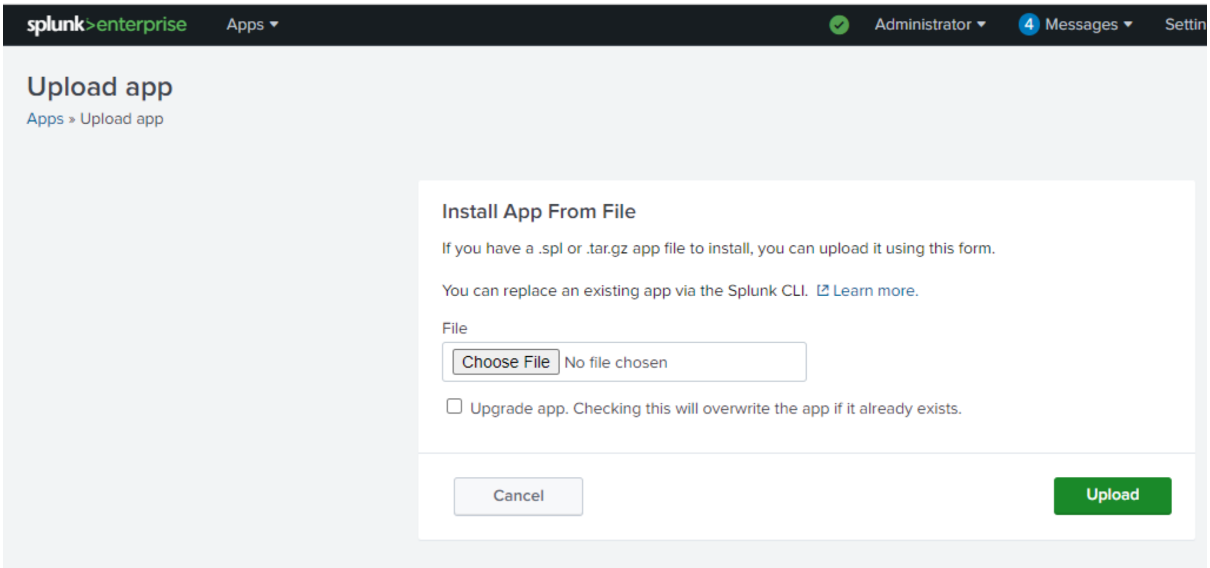
5.
6.



Apps

Showing 1-23 of 23 items

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
SplunkDeploymentServerConfig	SplunkDeploymentServerConfig		Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
SplunkForwarder	SplunkForwarder		Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App | Permissions	Disabled | Enable	
Log Event Alert Action	alert_logevent	9.4.7	Yes	No	App | Permissions	Enabled	Edit properties | View objects
Webhook Alert Action	alert_webhook	9.4.7	Yes	No	App | Permissions	Enabled	Edit properties | View objects
Apps Browser	appsbrowser	9.4.7	Yes	No	App | Permissions	Enabled	Edit properties | View objects
Audit Trail	audit_trail	1.0.0	Yes	Yes	App | Permissions	Enabled	Launch app | Edit properties | View objects
introspection_generator_addon	introspection_generator_addon	9.4.7	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
Home	launcher		Yes	Yes	App | Permissions	Enabled	Launch app | Edit properties | View objects
learned	learned		Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
legacy	legacy		Yes	No	App | Permissions	Disabled | Enable	
Upgrade Readiness App	python_upgrade_readiness_app	4.7.0	Yes	Yes	App | Permissions	Enabled | Disable	Launch app | Edit properties | View objects | Vie



Upload app

Apps » Upload app

Install App From File

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

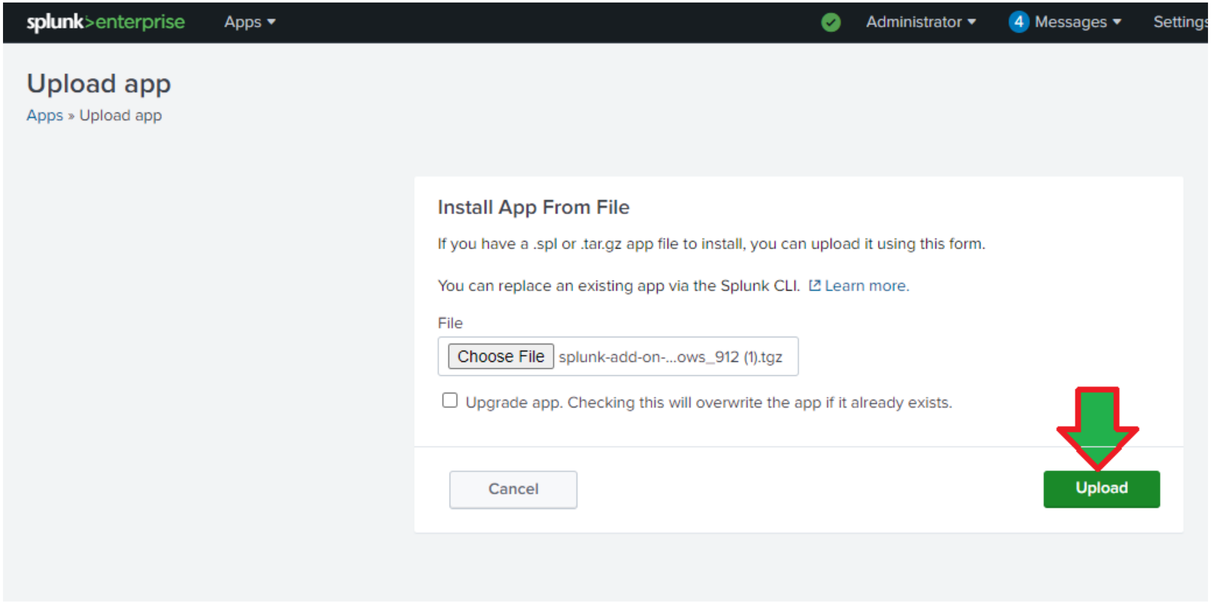
You can replace an existing app via the Splunk CLI. Learn more.

File

No file chosen

☐ Upgrade app. Checking this will overwrite the app if it already exists.

7.
8. Upload the .spl file



Upload app

Apps » Upload app

Install App From File

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

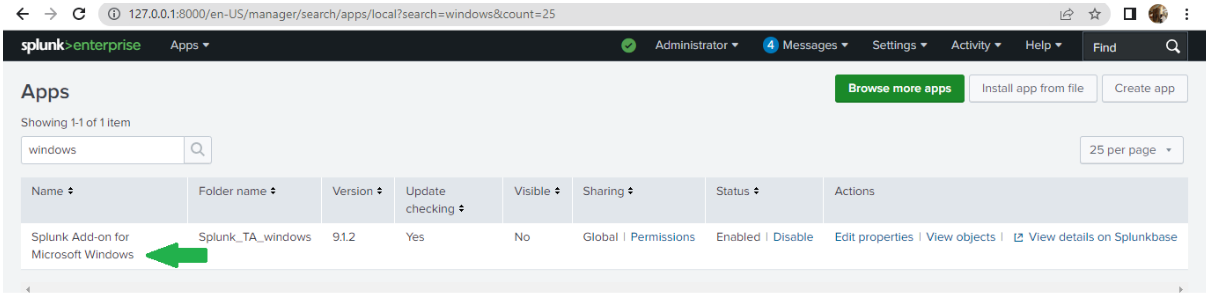
You can replace an existing app via the Splunk CLI. Learn more.

File

splunk-add-on-...ows_912 (1).tgz

☐ Upgrade app. Checking this will overwrite the app if it already exists.

9. Click **Install**



127.0.0.1:8000/en-US/manager/search/apps/local?search=windows&count=25

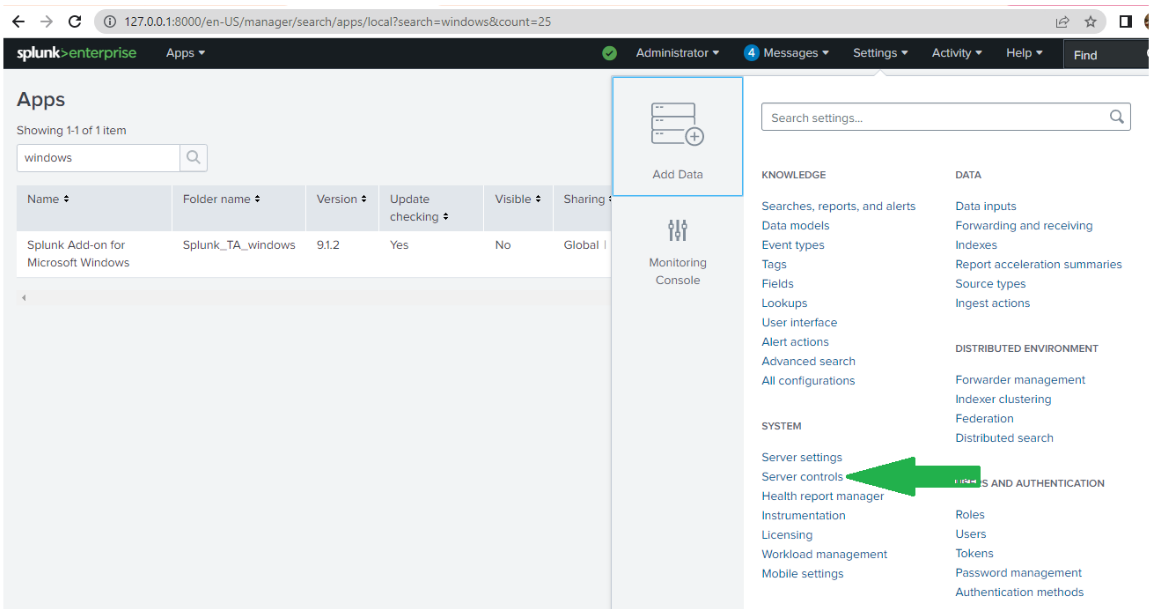
Apps

Showing 1-1 of 1 item

windows

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
Splunk Add-on for Microsoft Windows	Splunk_TA_windows	9.1.2	Yes	No	Global | Permissions	Enabled | Disable	Edit properties | View objects | View details on Splunkbase

10.


127.0.0.1:8000/en-US/manager/search/apps/local?search=windows&count=25

Apps

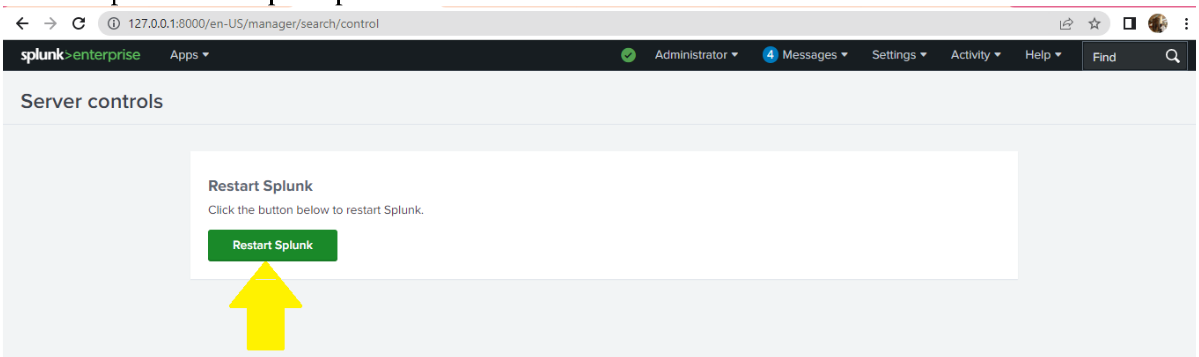
Showing 1-1 of 1 item

windows

Name	Folder name	Version	Update checking	Visible	Sharing
Splunk Add-on for Microsoft Windows	Splunk_TA_windows	9.1.2	Yes	No	Global

11.

12. Restart Splunk when prompted

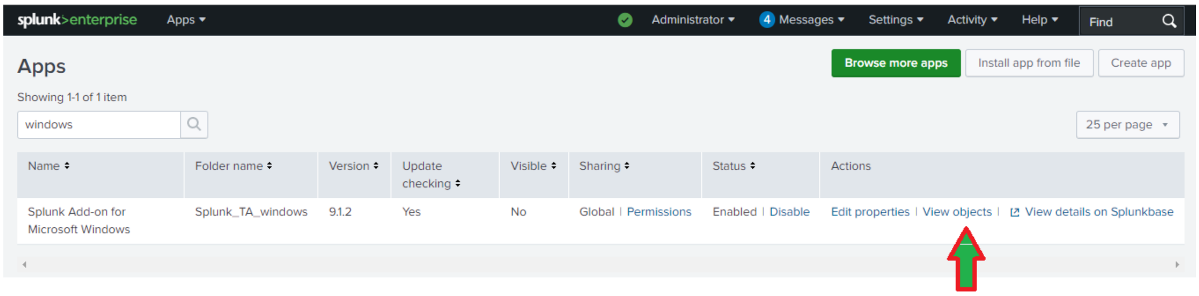

127.0.0.1:8000/en-US/manager/search/control

Server controls

Restart Splunk

Click the button below to restart Splunk.

13.



Apps

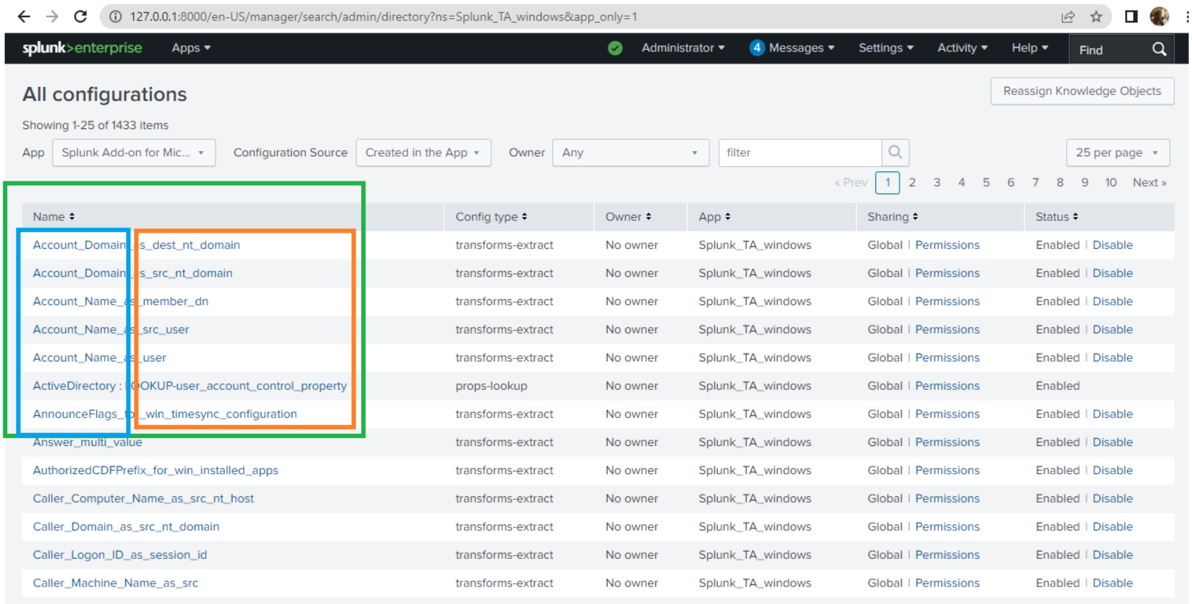
Showing 1-1 of 1 item

windows

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
Splunk Add-on for Microsoft Windows	Splunk_TA_windows	9.1.2	Yes	No	Global | Permissions	Enabled | Disable	Edit properties | View objects | View details on Splunkbase

14.

15.



127.0.0.1:8000/en-US/manager/search/admin/directory?ns=Splunk_TA_windows&app_only=1

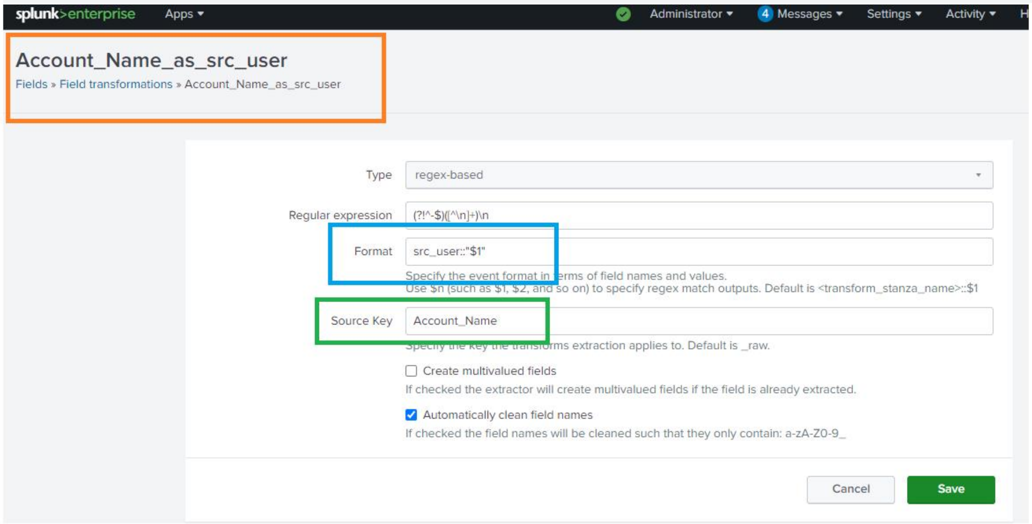
All configurations

Showing 1-25 of 1433 items

App: Splunk Add-on for Mic... ▾ Configuration Source: Created in the App ▾ Owner: Any ▾ filter 25 per page ▾

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Name ⬍	Config type ⬍	Owner ⬍	App ⬍	Sharing ⬍	Status ⬍
Account_Domain_as_dest_nt_domain	transforms-extract	No owner	Splunk_TA_windows	Global | Permissions	Enabled | Disable
Account_Domain_as_src_nt_domain	transforms-extract	No owner	Splunk_TA_windows	Global | Permissions	Enabled | Disable
Account_Name_as_member_dn	transforms-extract	No owner	Splunk_TA_windows	Global | Permissions	Enabled | Disable
Account_Name_as_src_user	transforms-extract	No owner	Splunk_TA_windows	Global | Permissions	Enabled | Disable
Account_Name_as_user	transforms-extract	No owner	Splunk_TA_windows	Global | Permissions	Enabled | Disable
ActiveDirectory : LOOKUP-user_account_control_property	props-lookup	No owner	Splunk_TA_windows	Global | Permissions	Enabled
AnnounceFlags_to_win_timesync_configuration	transforms-extract	No owner	Splunk_TA_windows	Global | Permissions	Enabled | Disable
Answer_multi_value	transforms-extract	No owner	Splunk_TA_windows	Global | Permissions	Enabled | Disable
AuthorizedCDFPrefix_for_win_installed_apps	transforms-extract	No owner	Splunk_TA_windows	Global | Permissions	Enabled | Disable
Caller_Computer_Name_as_src_nt_host	transforms-extract	No owner	Splunk_TA_windows	Global | Permissions	Enabled | Disable
Caller_Domain_as_src_nt_domain	transforms-extract	No owner	Splunk_TA_windows	Global | Permissions	Enabled | Disable
Caller_Logon_ID_as_session_id	transforms-extract	No owner	Splunk_TA_windows	Global | Permissions	Enabled | Disable
Caller_Machine_Name_as_src	transforms-extract	No owner	Splunk_TA_windows	Global | Permissions	Enabled | Disable



Account_Name_as_src_user

Fields » Field transformations » Account_Name_as_src_user

Type: regex-based

Regular expression: (?!^-$)([^\n]+)\n

Format: src_user::"$1"

Specify the event format in terms of field names and values.
Use $n (such as $1, $2, and so on) to specify regex match outputs. Default is <transform_stanza_name>::$1

Source Key: Account_Name

Specify the key the transforms extraction applies to. Default is _raw.

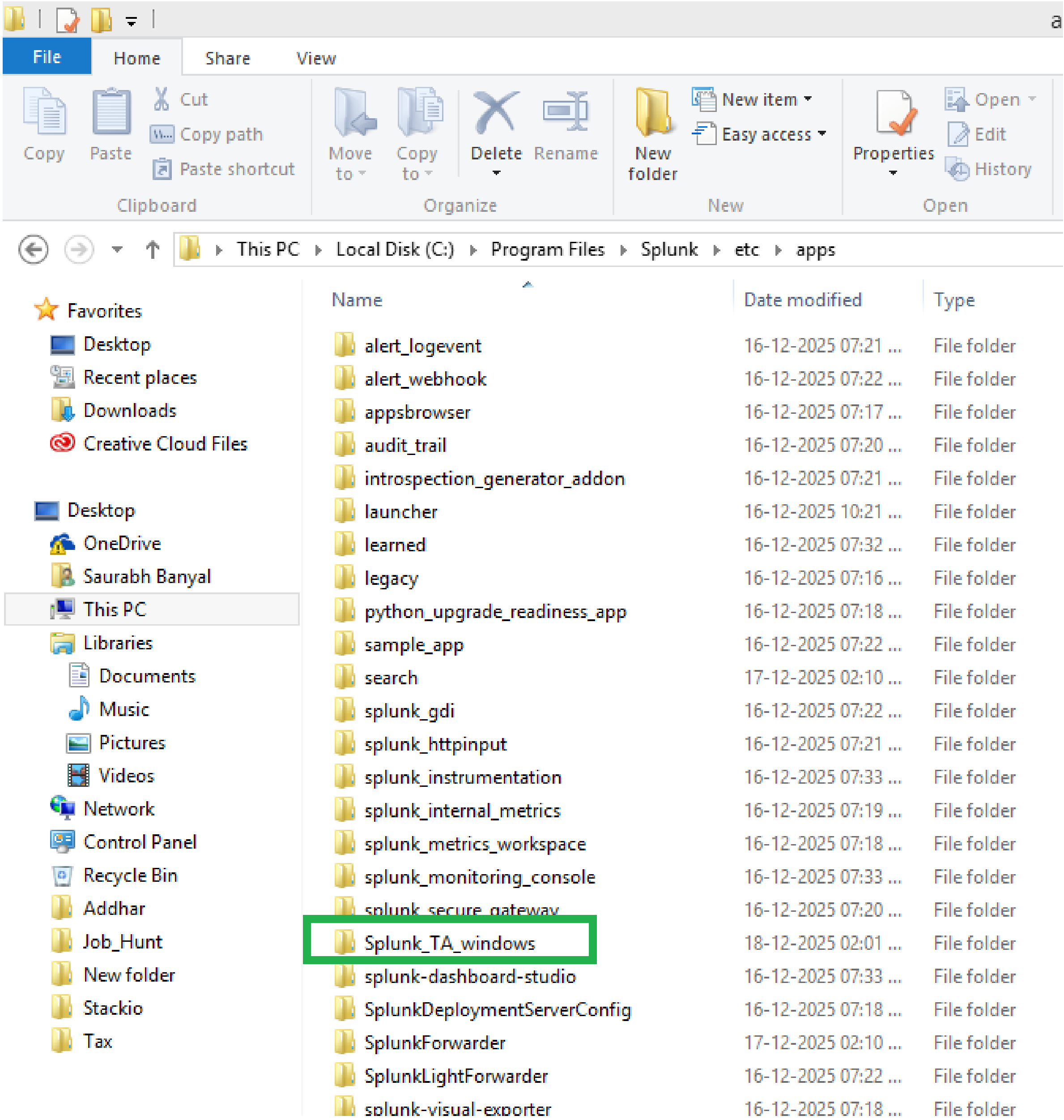
☐ Create multivalued fields

If checked the extractor will create multivalued fields if the field is already extracted.

☑ Automatically clean field names

If checked the field names will be cleaned such that they only contain: a-zA-Z0-9_

16.
17. BACKEND DIRECOTRY SRUCTURE
18. C:\Program Files\Splunk\etc\apps



This PC › Local Disk (C:) › Program Files › Splunk › etc › apps

Name	Date modified	Type
alert_logevent	16-12-2025 07:21 ...	File folder
alert_webhook	16-12-2025 07:22 ...	File folder
appsbrowser	16-12-2025 07:17 ...	File folder
audit_trail	16-12-2025 07:20 ...	File folder
introspection_generator_addon	16-12-2025 07:21 ...	File folder
launcher	16-12-2025 10:21 ...	File folder
learned	16-12-2025 07:32 ...	File folder
legacy	16-12-2025 07:16 ...	File folder
python_upgrade_readiness_app	16-12-2025 07:18 ...	File folder
sample_app	16-12-2025 07:22 ...	File folder
search	17-12-2025 02:10 ...	File folder
splunk_gdi	16-12-2025 07:22 ...	File folder
splunk_httpinput	16-12-2025 07:21 ...	File folder
splunk_instrumentation	16-12-2025 07:33 ...	File folder
splunk_internal_metrics	16-12-2025 07:19 ...	File folder
splunk_metrics_workspace	16-12-2025 07:18 ...	File folder
splunk_monitoring_console	16-12-2025 07:33 ...	File folder
splunk_secure_gateway	16-12-2025 07:20 ...	File folder
Splunk_TA_windows	18-12-2025 02:01 ...	File folder
splunk-dashboard-studio	16-12-2025 07:33 ...	File folder
SplunkDeploymentServerConfig	16-12-2025 07:18 ...	File folder
SplunkForwarder	17-12-2025 02:10 ...	File folder
SplunkLightForwarder	16-12-2025 07:22 ...	File folder
splunk-visual-exporter	16-12-2025 07:18 ...	File folder

19. [illegible]

◆

1. Another way , You can directly install on the location
2. C:\Program Files\Splunk\etc\apps

11. By unzipping the downloaded package from https://splunkbase.splunk.com/apps