



# **ArcSight User Behavior Analytics**

Software Version: 6.10

## Ingestion Node Installation Guide

4/17/2018

Powered by  **SECURONIX**

# Legal Notices

## Warranty

The only warranties for Micro Focus products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

Micro Focus ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

## Restricted Rights Legend

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

## Copyright Notice

© Copyright 2018 Micro Focus or one of its affiliates.

Follow this link to see a complete statement of copyrights and acknowledgments: <https://community.softwaregrp.com/t5/ArcSight-Discussions/Third-Party-Copyright-Notices-and-License-Terms/td-p/1589228>

## Legal Notice for Open Source Code

vLGPLv3, LGPLv2, EPL 1.0, CCDL

This product includes code licensed under the LGPLv3 licensed-code, LGPLv2 licensed-code, Eclipse Public License 1.0, CCDL-licensed code, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Micro Focus.

To obtain such source code on CD, send a check or money order in the amount of US \$10.00 (for shipping and handling) to:

Micro Focus

Attn: Gordon Lee

1140 Enterprise Way

Sunnyvale, CA 94089

USA

Please specify the product and version for which you are requesting the source code.

## Support

### Contact Information

Phone	A list of phone numbers is available on the Micro Focus ArcSight Technical Support Page: <a href="https://softwaresupport.softwaregrp.com/documents/10180/14684/esp-support-">https://softwaresupport.softwaregrp.com/documents/10180/14684/esp-support-</a>
-------	--

**Contact Information, continued**

	<a href="#">contact-list</a>
Support Web Site	<a href="https://softwaresupport.softwaregrp.com/">https://softwaresupport.softwaregrp.com/</a>
Protect 724 Community	<a href="https://community.softwaregrp.com/t5/Protect724/ct-p/Protect724">https://community.softwaregrp.com/t5/Protect724/ct-p/Protect724</a>

# Contents

---

<b>Deploying the Ingestion Node</b>	<b>5</b>
What is the Ingestion Node	5
Requirements for the Ingestion Node	5
Installing the Ingestion Node	6
Step 1: Command Line Installer	7
Step 1: GUI Installer	13
Step 2: Starting the Ingestion Node and Syslog Server	25
Step 3 - Verifying Ingestion Node Connectivity to Console	26
Stopping the Ingestion Node	28
<b>Troubleshooting the Ingestion Node</b>	<b>29</b>
Ingestion Node Installation Issues	29
Ingestion Node Post Installation Issues	29
Ingestion Node Log File for Troubleshooting	29
ArcSight UBA Console Issues	30
<b>Uninstalling the Ingestion Node</b>	<b>31</b>
<b>Appendix A - Configuring the Ingestion Node Properties Files</b>	<b>32</b>
Step 1: Generating the ingestercloud.properties file	32
Step 2: Configuring the SSL Keystores and Properties Files	33
Step 3: Verify the Remote ingestercloud.properties File	35

# Deploying the Ingestion Node

This section describes how you can deploy and configure the Ingestion Node to collect data.

## What is the Ingestion Node

The ArcSight Ingestion Node is a lightweight Java program that is used to forward logs in real time from remote servers to the ArcSight UBA Kafka brokers. This real-time forwarding of logs to Kafka brokers provides the ability to ingest and analyze events as soon as they are generated.

Using the Ingestion Node offers you the following advantages:

- Forwards logs from various data centers and locations
- Compresses the data to reduce network bandwidth utilization
- Encrypts data to secure the communications
- Maintains a local cache and retransmits data in case of communications failure

## Requirements for the Ingestion Node

The Ingestion Node has the following requirements:

### *Remote Ingestion Node (RIN) Server Requirements*

The Remote Ingestion Node (RIN) is a lightweight process that collects and forwards logs to the ArcSight UBA centralized Kafka Brokers. Several Remote Ingestion Nodes can be deployed in remote locations to collect and forward the events to ArcSight UBA. The RIN servers can be physical servers or virtual machines. The following table describes the RIN sizing recommendations for a small, medium and large configuration.

### *Remote Ingestion Node Sizing Recommendations*

	Small (1000 EPS)	Medium (5000 EPS)	Large (10000 EPS)
CPU	4	6	8
Memory (GB)	8	16	64
Storage (/Securonix)	100 GB	1 TB	2 TB



**Note:** A 10 GB network is recommended for more than 1000 EPS.

The sizing recommendations are made on the following assumptions:

- Operating System: CentOS 7.x or Red Hat 7.x
- Data Retention on the RIN: 4 days



**Note:** Additional storage can be added if the data retention on the RIN server is longer than 4 days.

- Additional CPUs may be required if a large number of jobs are scheduled on the RIN

### Firewall Configuration

Source	Destination
RIN Server	ArcSight UBA Consoles (typically port 80 or 443)
RIN Server	Kafka Brokers (typically port 9092 or 9093)
Syslog sources	RIN syslog server (port 514 typically)

### Non-root User Requirements

The ArcSight UBA Remote Installer should be installed by a non-root user. To create a non-root user, open a terminal session and run the following commands:

1. `useradd securonix` (For example, choose any user name.)
2. `passwd securonix` (Provide your non-root user a password.)
3. Log in as root and go to `/etc/`  
`vi sudoers`
4. Scroll down through the sudoers file to the section below, add the user information for the non-root user that will start the installer (securonix from the example above), and save the file. Provide the non-root user password as sudo password on the installer screen.

```
## Allow root to run any commands anywhere
root ALL=(ALL) ALL
securonix ALL=(ALL) ALL
## Allows members of the 'sys' group to run networking,
software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE,
DELEGATING, PROCESSES, LOCATE, DRIVERS
## Allows people in group wheel to run all commands
```

## Installing the Ingestion Node

Install the Ingestion Node using either of the following methods: [Step 1: Command Line Installer](#) or the [Step 1: GUI Installer](#).

After installing the Ingestion Node using one of the installer options, go to [Step 2: Starting the Ingestion Node and Syslog Server](#).

## Step 1: Command Line Installer

Once you have downloaded the installation file for the Ingester, follow these steps to install it:

1. Download the installation file and transfer the file to the Ingestion Node server.
2. Create the /Securonix folder with ownership assigned to the **securonix** account.

```
mkdir /Securonix  
chown securonix:securonix /Securonix
```



**Note:** Create the /Securonix folder under the / folder. This is required as syslog is deployed under /Securonix.

3. Ensure that you are installing the ArcSight\_UBA\_6.10\_Ingestion\_Node\_xxxxxxx.bin as user **securonix**. As a root user, execute the following commands to create a /Securonix folder to make the ArcSight\_UBA\_6.10\_Ingestion\_Node\_xxxxxxx.bin an executable for the **securonix** user:

```
chown securonix:securonix ArcSight_UBA_6.10_Ingestion_Node_XXXXXXX.bin  
chmod u+x ArcSight_UBA_6.10_Ingestion_Node_XXXXXXX.bin
```

The /Securonix folder must be created under / and owned by the **securonix** user. This is required as syslog is deployed under /Securonix.

4. Launch the installer as **securonix** user with this command:

```
./ArcSight_UBA_6.10_Ingestion_Node_xxxxxxx.bin
```

```
Configuring the installer for this system's environment...

Launching installer...

=====
ArcSight User Behavior Analytics Ingestion Node Installer(created with InstallAnywhere)
=====

Preparing CONSOLE Mode Installation...

=====
Introduction
=====

InstallAnywhere will guide you through the installation of ArcSight User
Behavior Analytics Ingestion Node Installer.

It is strongly recommended that you quit all programs before continuing with
this installation.

Respond to each prompt to proceed to the next step in the installation. If
you want to change something on a previous step, type 'back'.

You may cancel this installation at any time by typing 'quit'.

NOTE: You need to have a directory /Securionix and it should have right
permissions as syslog will be installed under /Securionix/syslog

[PRESS <ENTER> TO CONTINUE:
```

5. Confirm that the /Securionix folder is created with the correct permissions.

```
=====
Important Information
=====

Please read before continuing:

Server Prerequisites:
* Make sure you have /Securionix directory created under / and it is owned by
the non-root user who is running this installer. This is required as syslog
will be deployed under /Securionix

IMPORTANT INFORMATION COMPLETE. PRESS <ENTER> TO CONTINUE: █
```

6. Accept the license agreement, and click **Enter** to continue.



```
non-performance due to causes beyond its reasonable control, except for
payment obligations.

i. Entire Agreement. This Agreement represents our entire understanding with
respect to its subject matter and supersedes any previous communication or
agreements that may exist. Modifications to the Agreement will be made only
through a written amendment signed by both parties. If Micro Focus doesn't
exercise its rights under this Agreement, such delay is not a waiver of its
rights.

[PRESS <ENTER> TO CONTINUE:]

16. Australian Consumers. If you acquired the software as a consumer within
the meaning of the 'Australian Consumer Law' under the Australian Competition
and Consumer Act 2010 (Cth) then despite any other provision of this Agreement,
the terms at this URL apply: https://software.microfocus.com/about/software-licensing.

17. Russian Consumers. If you are based in the Russian Federation and the
rights to use the software are provided to you under a separate license and/or
sublicense agreement concluded between you and a duly authorized Micro Focus
partner, then this Agreement shall not be applicable.

[PRESS <ENTER> TO CONTINUE:]

5200-0949 v1.0, 2018

(c) Copyright 2015-2018 EntIT Software LLC

DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N): █
```

7. Choose the path to the installation folder.  
For example: /Securonix/ArcSightIngester

```

=====
Choose Install Folder
=====

Provide a destination folder for the installation. Remote ingester will be
deployed at this location during the installation.

Provide a destination folder for the installation

    Default Install Folder: /Securonix/ArcSightIngester

ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
[      ] :

```

8. Enter the sudo password.

```

=====
Enter SUDO Password
=====

This installation requires sudo password to continue. SUDO password is the
password of non-root user which is included in the sudoers file.
If this user doesn't have SUDO password leave this field blank and press ENTER
to proceed.

[Please Enter the Password:

```

9. Enter the ArcSight UBA Console access instructions.



**Note:** The ArcSight UBA Console must be running and accessible on the network from the server where the RIN is installed.

The following steps create a shared secret in an encrypted properties file for the RIN to access the web services of the ArcSight UBA Console.

Enter the ArcSight UBA Console details:

URL (example: <https://10.0.0.100:8443/Snypr>)

Admin user (example: admin)

Admin password (example: adminpw123 )

```

=====
ArcSight UBA Application Details
=====

Enter ArcSight_UBA Application url

[ArcSight_UBA Application url (Default: )]: https://10.0.51.198:8446/Snypr

=====

ArcSight UBA Application Details
=====

Enter ArcSight_UBA Application username

[ArcSight_UBA Application username (Default: )]: admin

=====

ArcSight UBA Application Details
=====

Enter ArcSight_UBA Application Password

[Please Enter ArcSight_UBA Application Password:

```

If the steps fail, refer to [Troubleshooting the Ingestion Node](#). Post-installation configuration is required if the Kafka brokers are protected with SSL or if the ArcSight UBA Console is configured for SSL using a self-signed certificate.

10. Select the event broker if it is available, and provide the bootstrap server information.

```

=====
ArcSight Event Broker
=====

Is Arcsight Event Broker available?
NOTE : ArcSight Event Broker is the kafka topic from which the data will be
pulled in the application.

    1- Available
    ->2- Not_Available

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:: 1

```

1. **Available:** Provide the bootstrap server information for the event broker.

```
=====
ArcSight Event Broker Details
=====

Enter the Kafka Broker details (bootstrap server) of the ArcSight Event
Broker
INFO : Bootstrap servers is a comma-separated list of host and port pairs that
are the addresses of the Kafka brokers in a "bootstrap" Kafka cluster that a
Kafka client connects to initially to bootstrap itself. A host and port pair
uses : as the separator.
Bootstrap Servers (Format: 10.x.x.x:9092, 192.168.x.x:9092)
or (Format: HOSTNAME1:9092,HOSTNAME2:9092,HOSTNAME3:9092) If you are using
HOSTNAME make sure it is in /etc/hosts file.

[Bootstrap servers (Default: ): 34.224.90.226:9092
```

2. **Not Available:** Proceed to **Step 12: Confirm Pre-Installation Summary.**

11. Select **NOT\_SSL\_ENABLED** to be directed to the Pre-Installation Summary.

```
=====
SSL Info for AEB
=====

Is Arcsight Event Broker topic SSL Enabled?

1- SSL_ENABLED
->2- NOT_SSL_ENABLED

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:: 1
```

12. Confirm the Pre-Installation Summary to continue.

```
=====
Pre-Installation Summary
=====

Please review the following information before you continue:

Product Name:
  ArcSight User Behavior Analytics Ingestion Node Installer

Install Folder:
  /Securonix/ArcSightIngester

Product Features:
  Ingester

Disk Space Information (for Installation Target):
  Required: 0.29 GigaBytes
  Available: 50.26 GigaBytes

PRESS <ENTER> TO CONTINUE: 
```

- Exit the installer when the application is successfully installed.

```

=====
Installation Complete
=====

ArcSight User Behavior Analytics Ingestion Node Installer  installation
completed successfully.

Thank you for installing ArcSight User Behavior Analytics Ingestion Node
Installer.

NOTE: Execute following command after installation
. ~/.bash_profile
Please start ingester service as a NON_ROOT USER ONLY using the command:
service scnx-ingester start
Please start syslog-ng service using the command:
For non-root user - sudo service scnx-syslog-ng start
For root user - service scnx-syslog-ng start
Please start arcsight_eb_to_securonix service as NON_ROOT USER using the
command: service scnx-arcsight_eb_to_securonix start
NOTE:
To check the logs for ingester
tail -1234f
/Securonix/ArcSightIngester/Ingester/service/scnx-ingester/scnx-ingester.log
To check the logs for syslog-ng
tail -1234f /var/log/syslog-ng/syslog-ng.log
To check the logs for arcsight_eb_to_securonix
tail -1234f /Securonix/ArcSightIngester/Ingester/ArcsightEB2Securonix/service/
arcsight_eb_to_securonix

NOTE: If Kafka is SSL enabled, please set up the SSL . Please refer the
documentation for steps to configure SSL.

PRESS <ENTER> TO EXIT THE INSTALLER: █

```

- Execute `bash_profile` and validate the `Ingester_Home` by using the following commands:

```

source ~/.bash_profile
echo $INGESTER_HOME

```

## Step 1: GUI Installer

Once you have downloaded the installation file for the Ingester, follow these steps to install it:

- Download the installation file and transfer the file to the Ingestion Node server.
- Create the `/Securonix` folder with ownership assigned to the **securonix** account.

```

mkdir /Securonix
chown securonix:securonix /Securonix

```



**Note:** Create the `/Securonix` root under the `/` folder. This is required as syslog is deployed under `/Securonix`.

- Ensure that you are installing the `ArcSight_UBA_6.10_Ingestion_Node_xxxxxxx.bin` as user **securonix**. As a root user, execute the following commands to create a `/Securonix` folder to

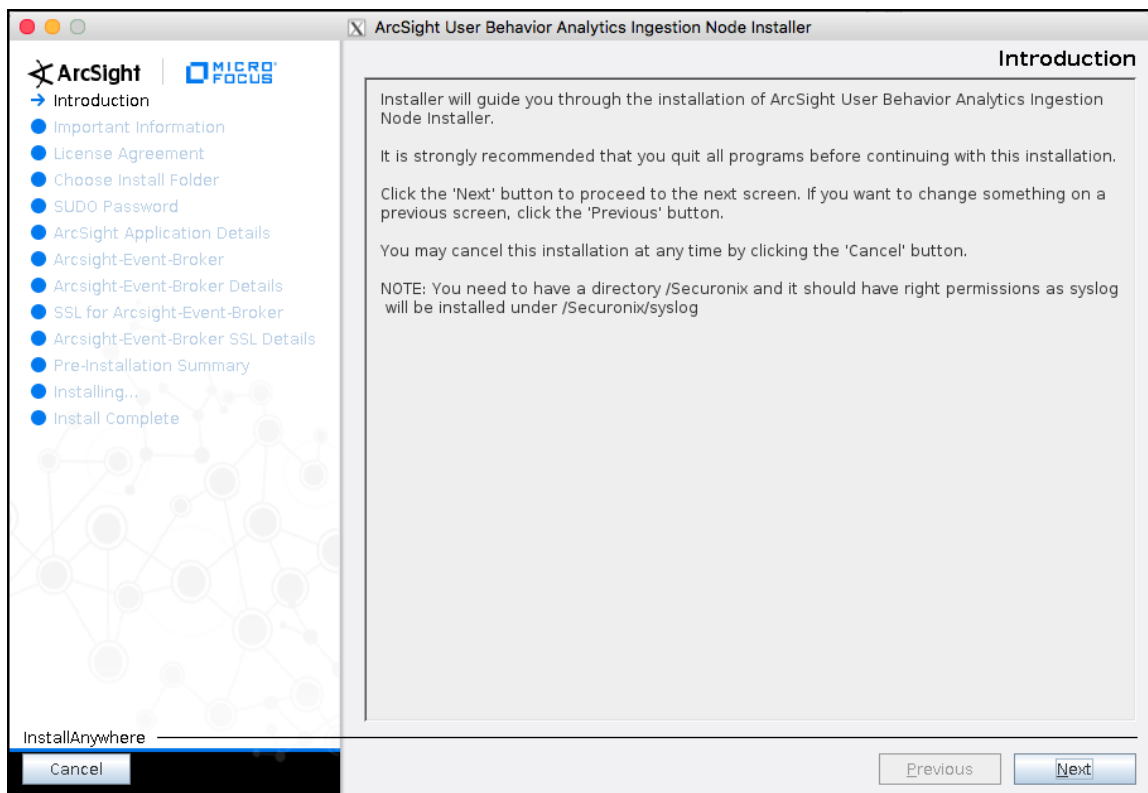
make the ArcSight\_UBA\_6.10\_Ingestion\_Node\_XXXXXXX.bin an executable for the **securonix** user:

```
chown securonix:securonix ArcSight_UBA_6.10_Ingestion_Node_XXXXXXX.bin
chmod u+x ArcSight_UBA_6.10_Ingestion_Node_XXXXXXX.bin
```

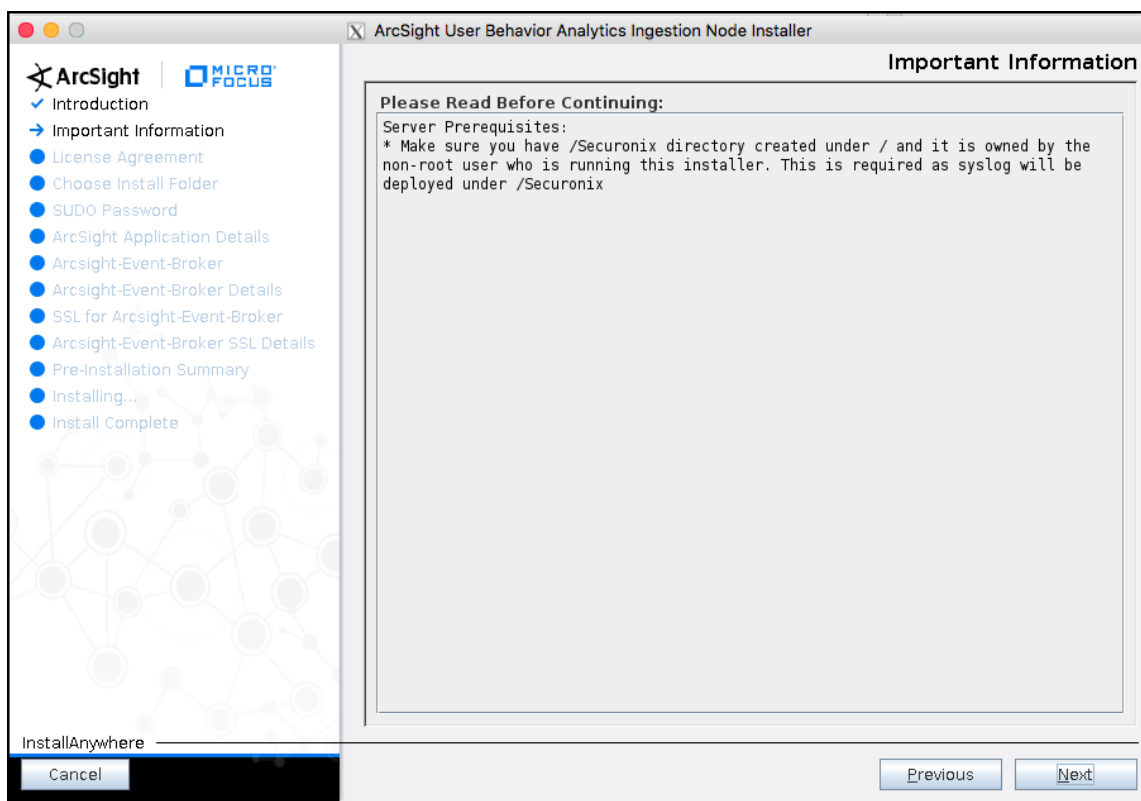
The /Securonix folder must be created under / and owned by the **securonix** user. This is required as syslog is deployed under /Securonix.

4. Launch the installer as **securonix** user with this command, and click **Next**:

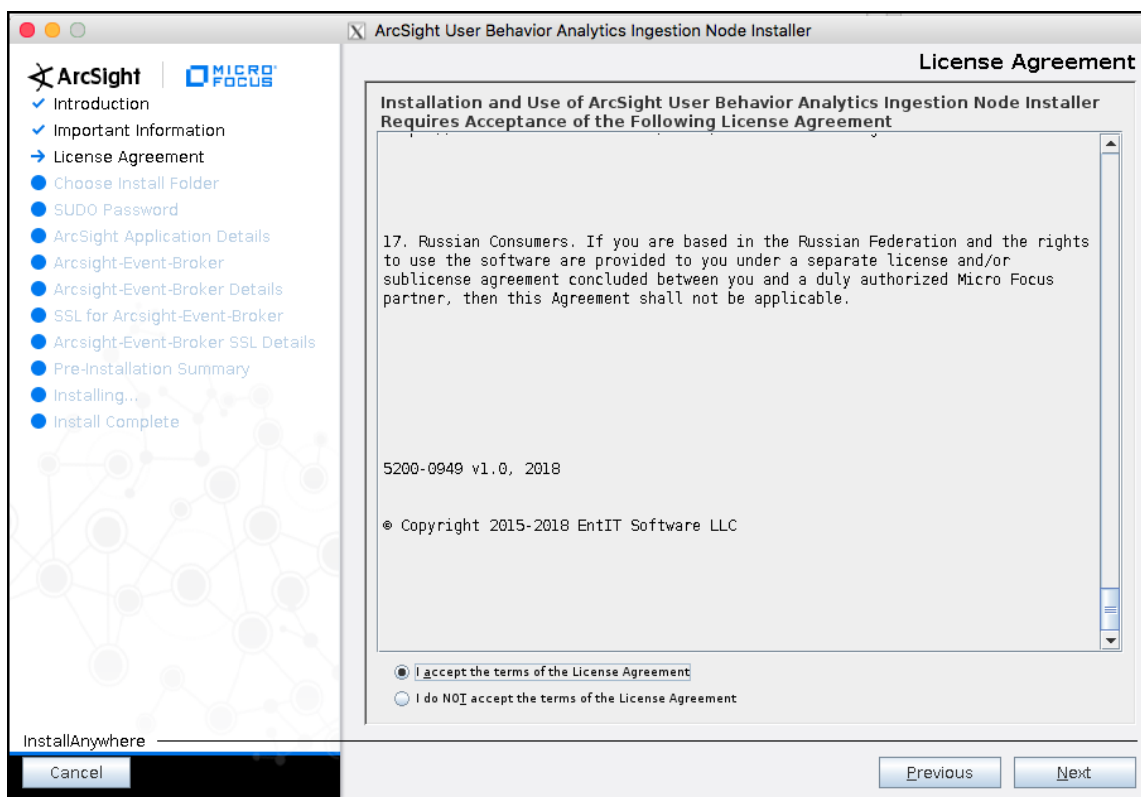
```
./ArcSight_UBA_6.10_Ingestion_Node_XXXXXXX.bin
```



5. Confirm that the /Securonix folder is created with the correct permissions, and click **Next**.



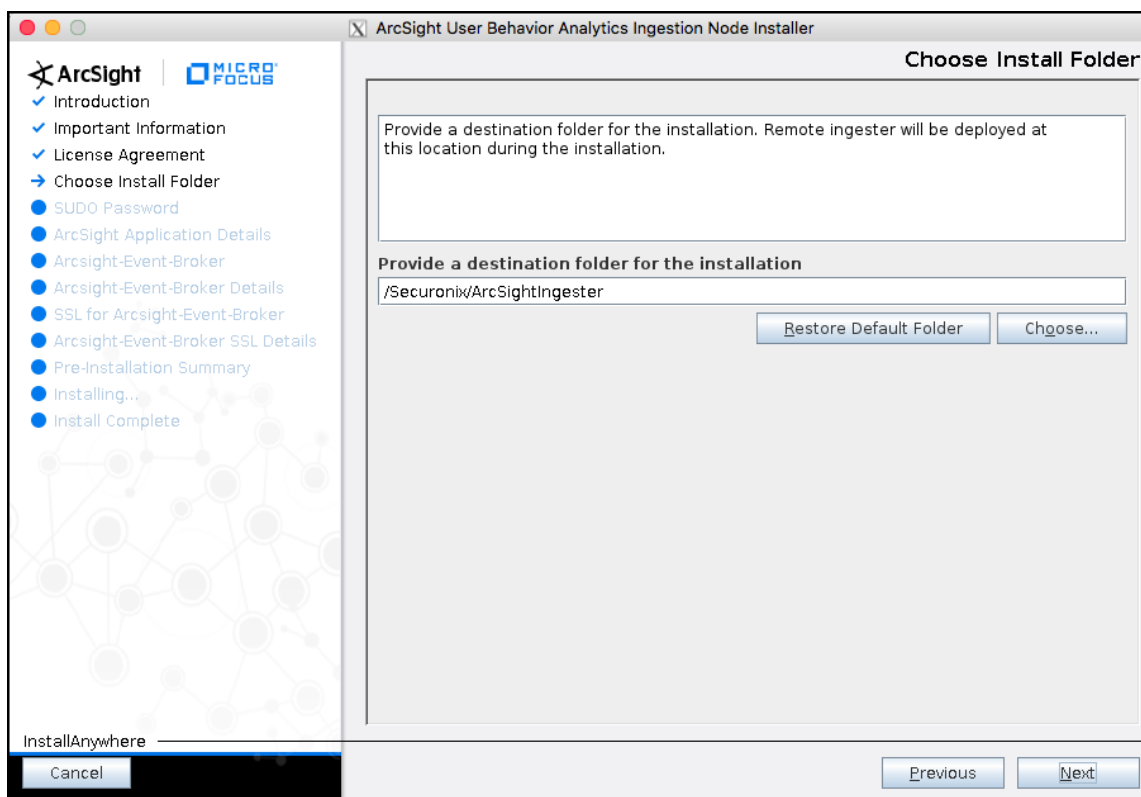
6. Accept the license agreement, and click **Next** to continue.



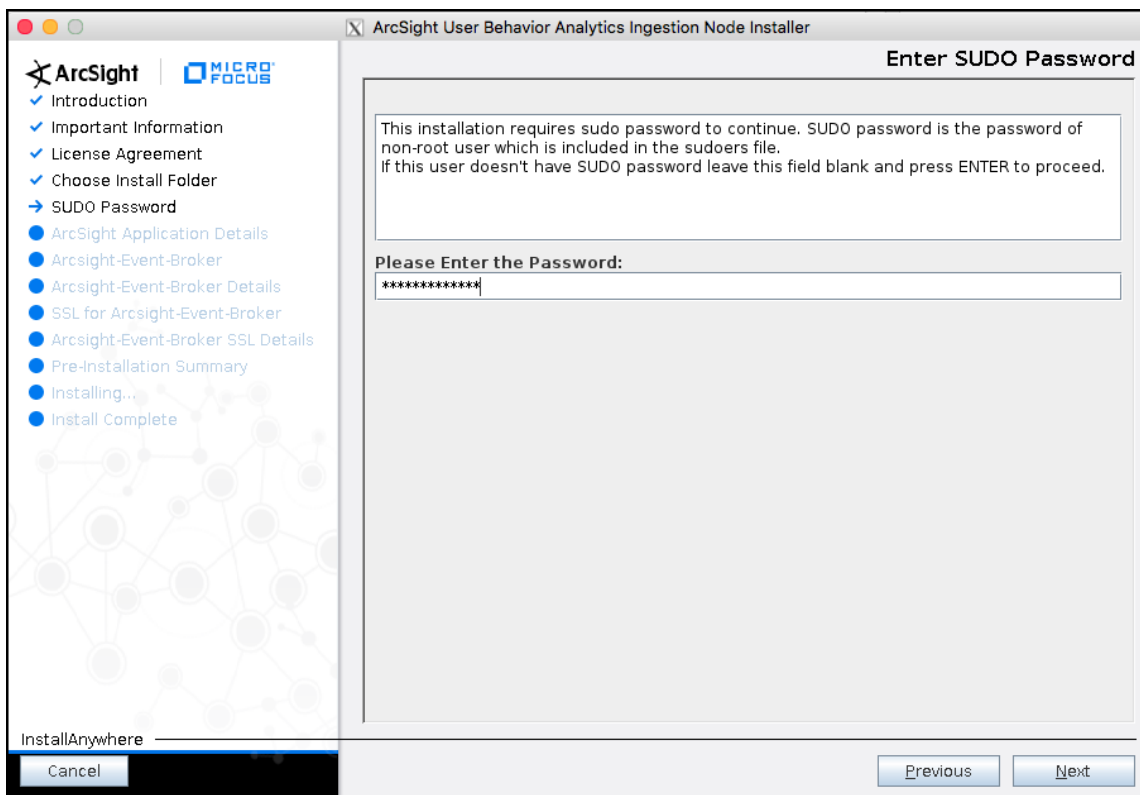
7. Choose the path to the installation folder, and click **Next**.

For example: /Securonix/ArcSightIngester





8. Enter the sudo password.



9. Enter the ArcSight UBA Console access instructions.

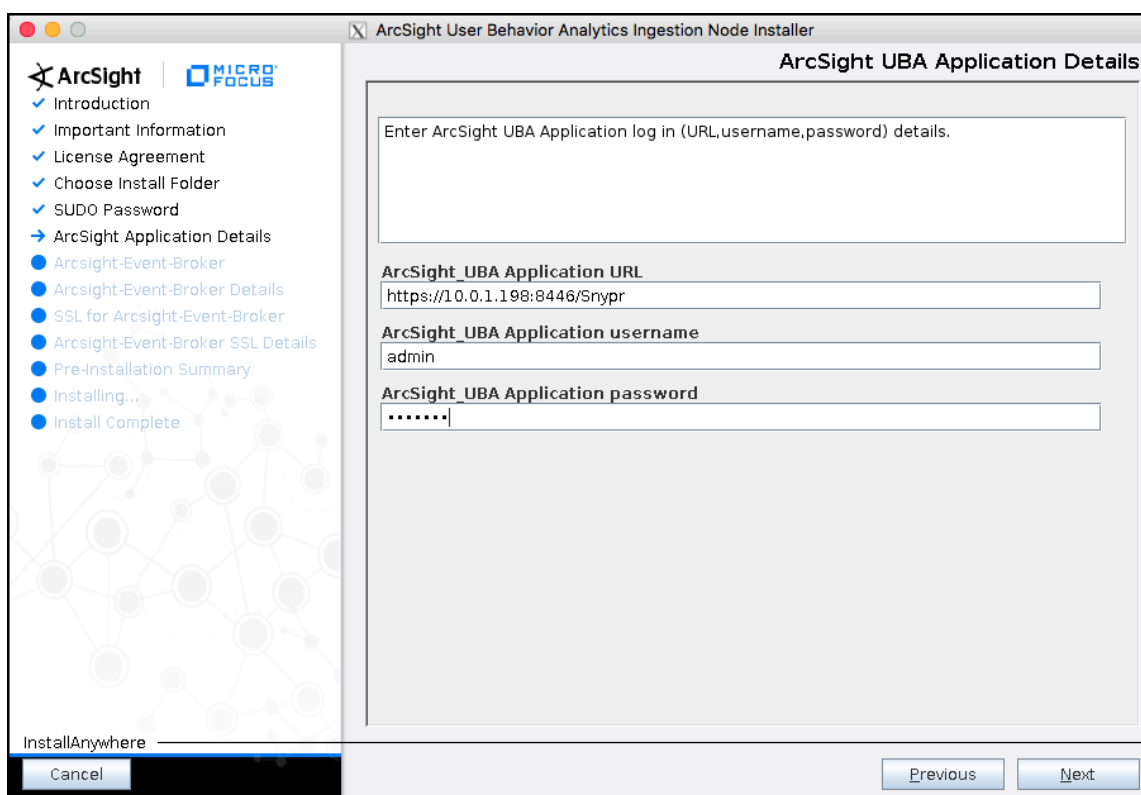


**Note:** The ArcSight UBA Console must be running and accessible on the network from the server where the RIN is installed.

The following steps create a shared secret in an encrypted properties file for the RIN to access the web services of the ArcSight UBA Console.

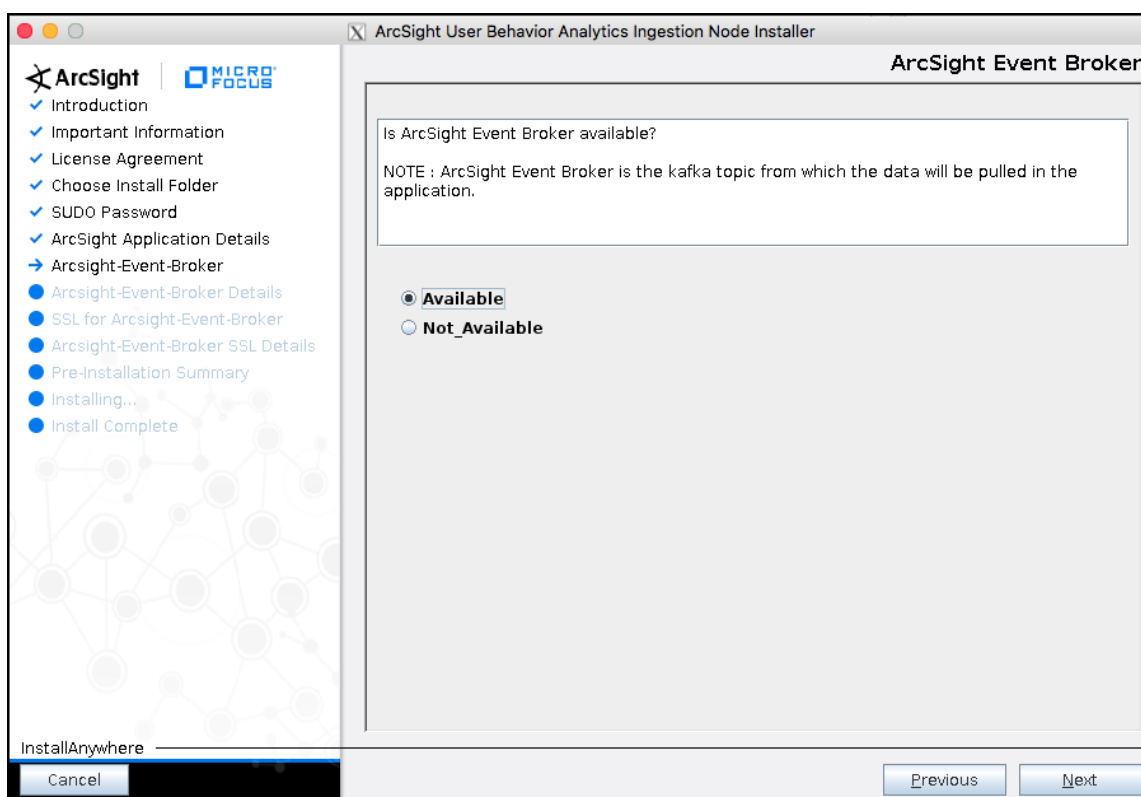
Enter the ArcSight UBA Console details:

- URL (example: <https://10.0.0.100:8443/Snypr>)
- Application user name (example: admin)
- Application password (example: adminpw123)



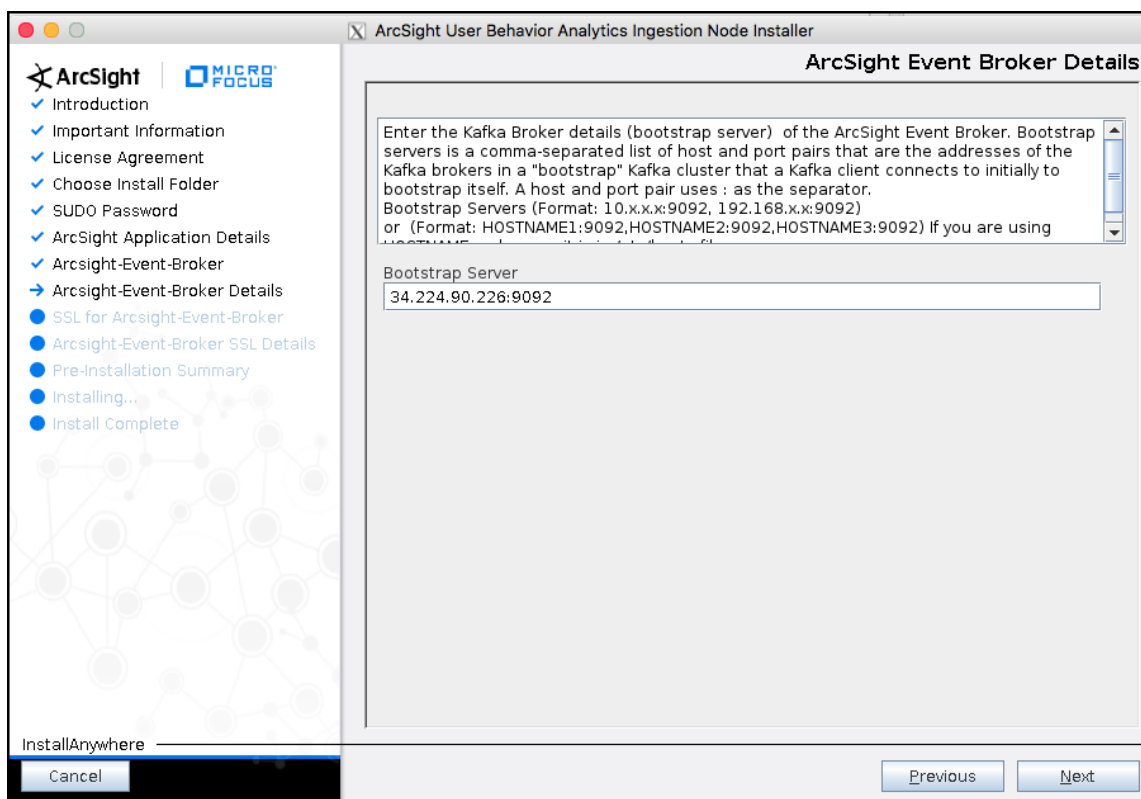
If the step fails, the Ingestion Node installation will continue. After installing the Ingester, refer to [Appendix A](#) for post installation configuration. Post-installation configuration is required if the Kafka brokers are protected with SSL or if the ArcSight UBA Console is configured for SSL using a self-signed certificate.

10. Indicate if the event broker is available.

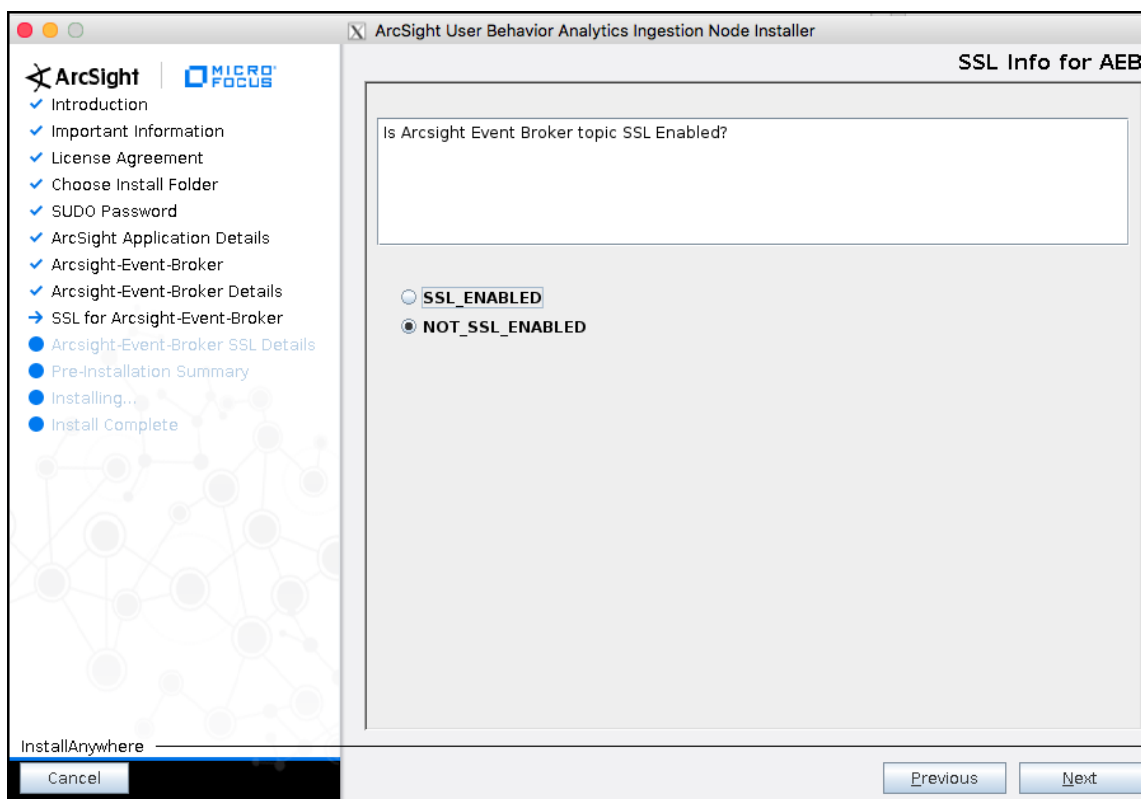


If the ArcSight Event Broker is SSL enabled, and SSL is not enabled in your environment, follow the steps described in [Appendix A - Configuring the Ingestion Node Properties Files](#) to configure the SSL keystores and properties files after installation.

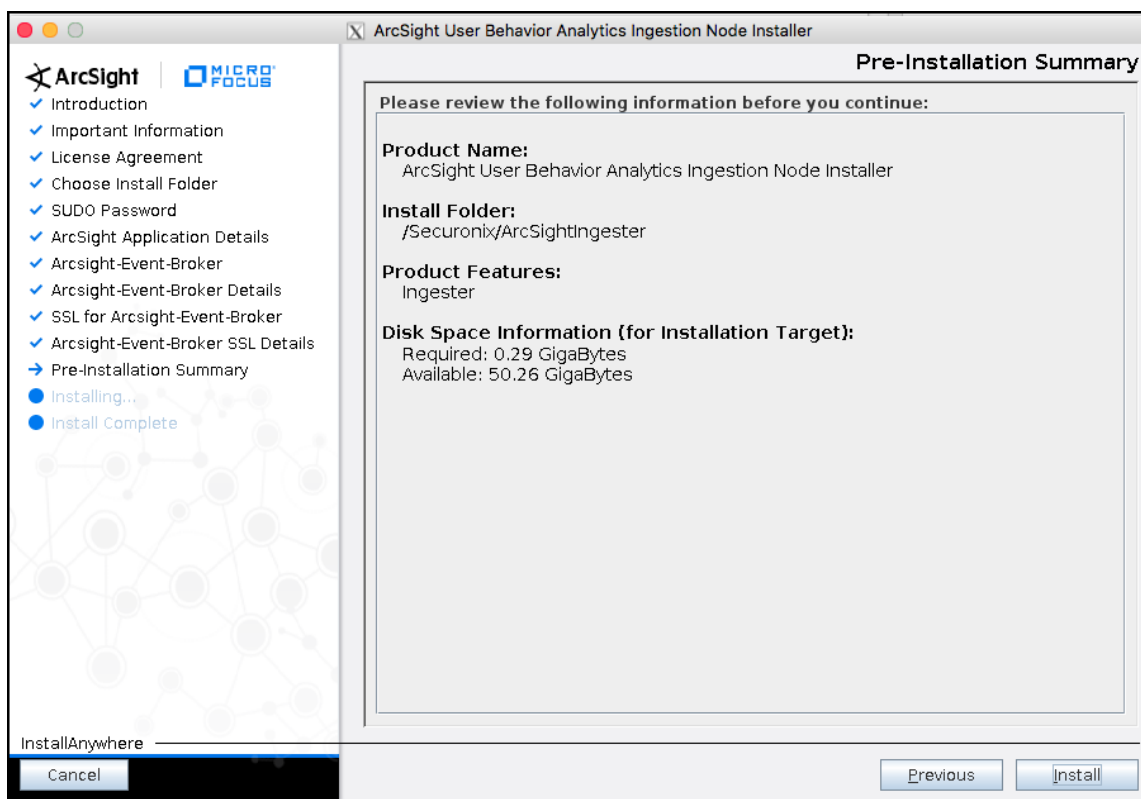
11. Provide the bootstrap server information for the event broker.



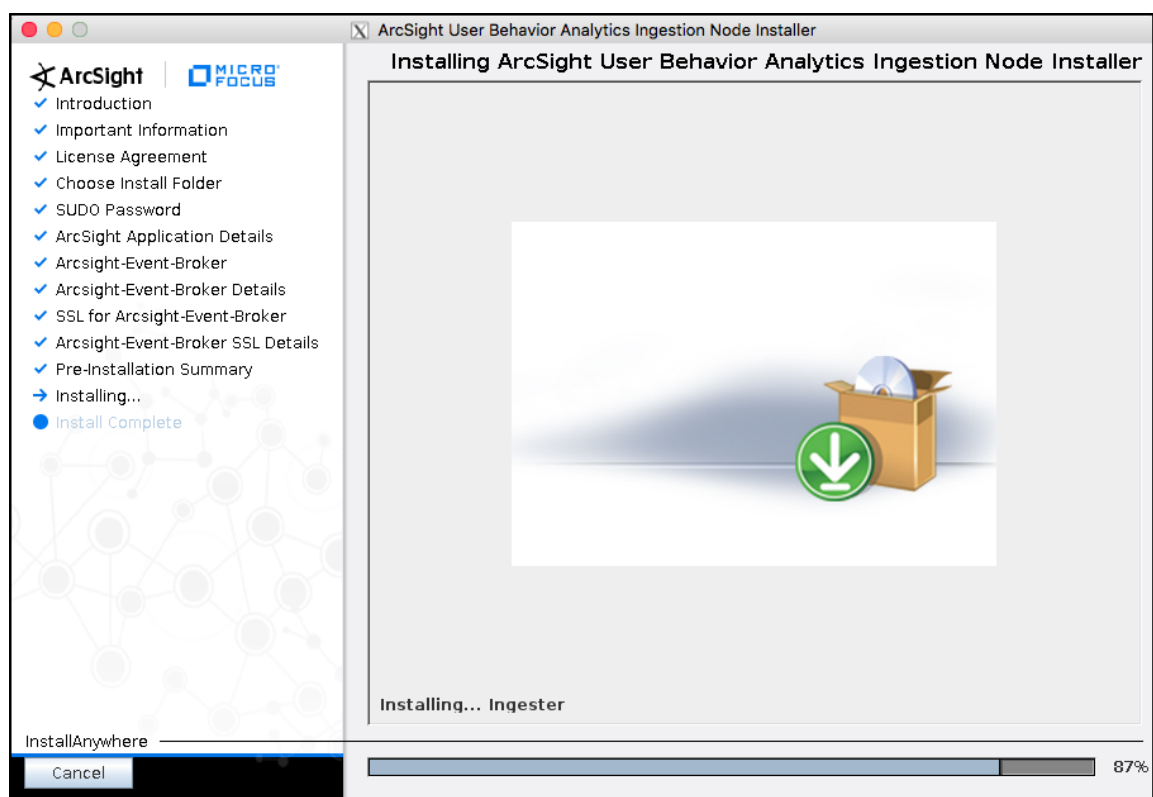
12. Select **NOT\_SSL\_ENABLED**.



13. Review the pre-installation summary and click **Install** to proceed.

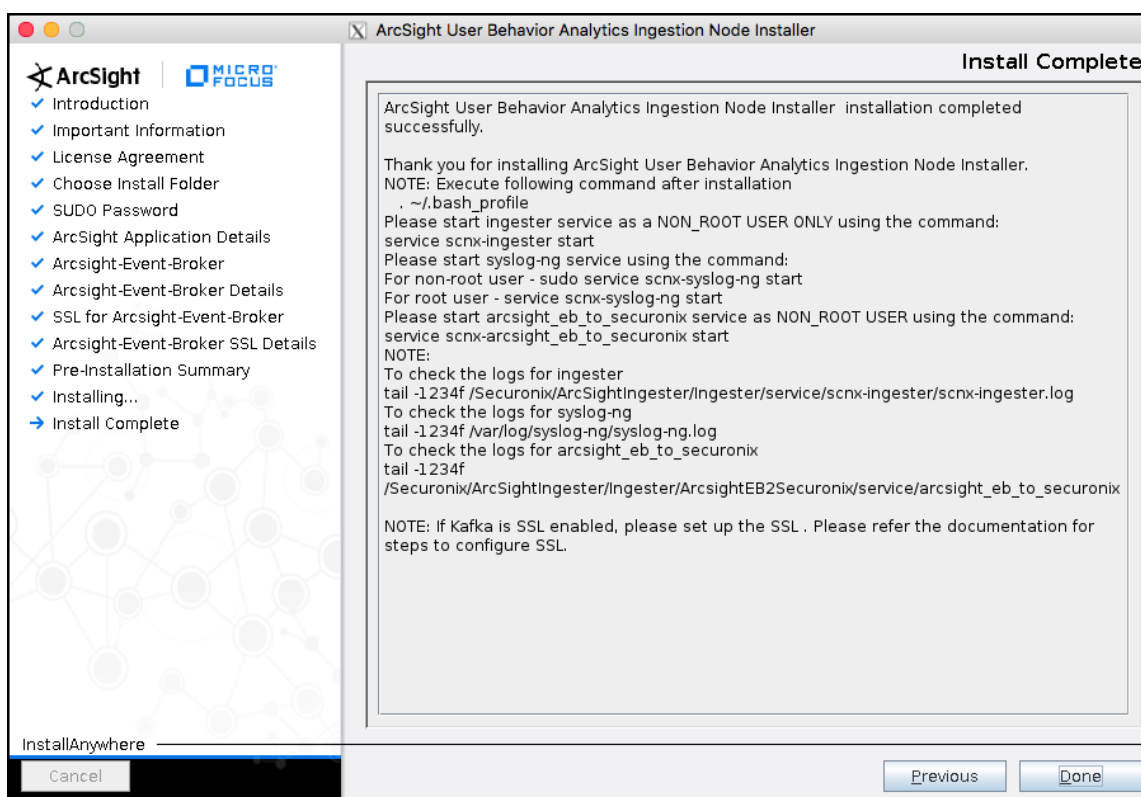


The installation will begin.



14. Click **Done** to complete the installation.





15. Execute `bash_profile` and validate the `Ingestion_Home` by using the following commands:

```
source ~/.bash_profile
echo $INGESTER_HOME
```



**Note:** Post-installation configuration is required if the Kafka brokers are protected with SSL or if the ArcSight UBA Console is configured for SSL using a self-signed certificate. Refer to [Appendix A](#) for the post-installation configuration.

## Step 2: Starting the Ingestion Node and Syslog Server

Follow these steps to start the Ingestion Node and the Syslog Service:

1. Start the Ingestion Node as **securedix** user using the following command:
 

```
service scnx-ingester start
```
2. Check the Ingestion Node status with the following command to confirm that it has started:
 

```
service scnx-ingester status
```

If there is an error or you want to check the Ingestion Node logs, use this command:

```
tail -1234f /<your_installation_path>/Ingestion/service/scnx-ingester/scnx-ingester.log
```
3. Start the Syslog server using the following command:

- As a **securonix** user:

```
sudo service scn-x-syslog-ng start
```

To stop or check the status of the Syslog server:

```
sudo service scn-x-syslog-ng stop
sudo service scn-x-syslog-ng status
```

To check the logs for the Syslog server:

```
/var/log/syslog-ng/syslog-ng.log
```

- As a root user:

```
service scn-x-syslog-ng start
```

To stop or check the status of the Syslog server:

```
service scn-x-syslog-ng stop
service scn-x-syslog-ng status
```

If you have ArcSight Event Broker in your environment, complete the following steps:

1. Start `arcsight_eb_to_securonix` service as **securonix** using the following command:

```
service scn-x-arcsight_eb_to_securonix start
```

2. Use the following commands to stop or check the status of the `arcsight_eb_to_securonix` service:

```
service scn-x-arcsight_eb_to_securonix stop
service scn-x-arcsight_eb_to_securonix status
```

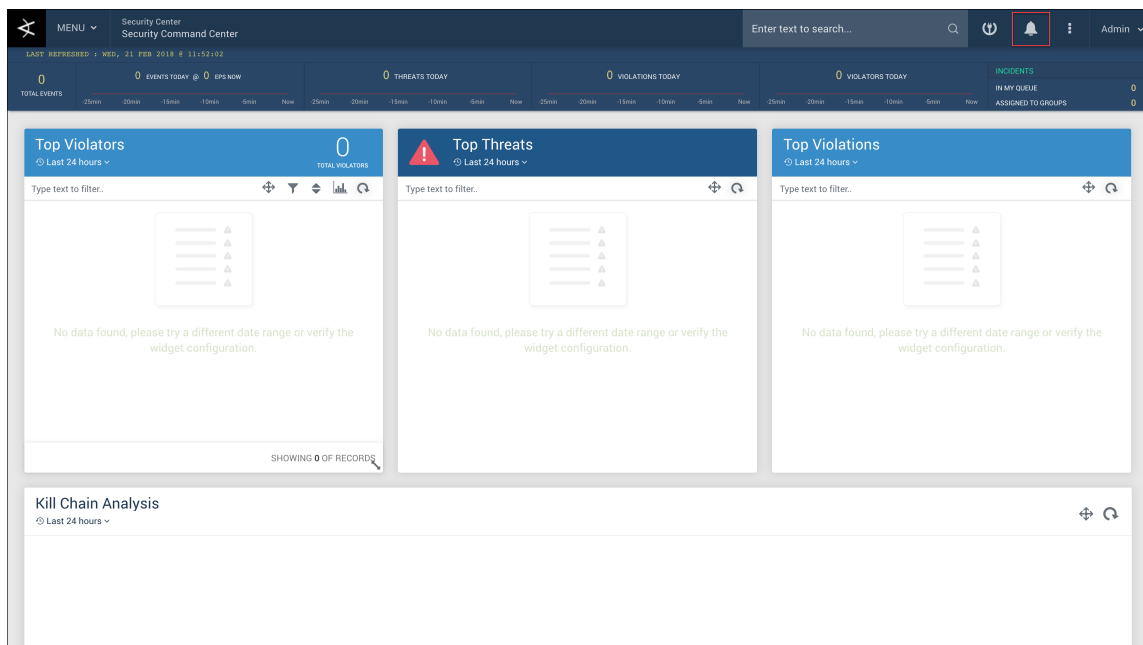
3. Use the following commands to check the logs for `arcsight_eb_to_securonix`:

```
tail -1234f /<your_installation_path>/Ingester/ArcsightEB2Securionix/service/arcsight_eb_to_securonix/arcsight_eb_to_securonix.log
```

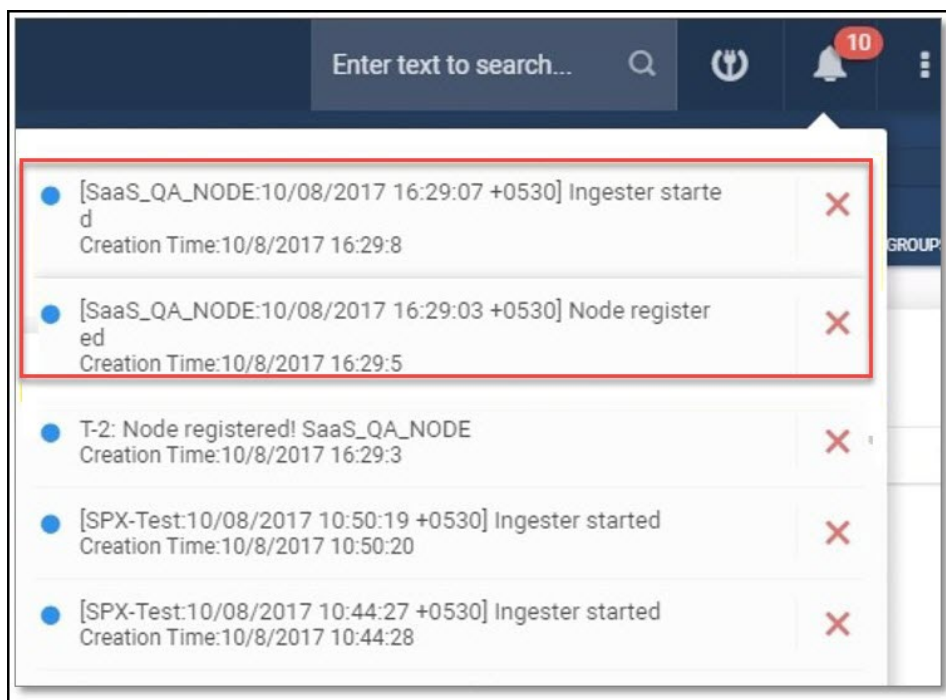
## Step 3 - Verifying Ingestion Node Connectivity to Console

When the Ingestion Node starts, it tries to validate the token with the application. If the connection is successful, you are prompted with a message that says Token Validated. If the connection fails, the Ingestion Node shuts down.

Upon logging into the web console, click the notification icon to ensure the connection is successful.



The Ingester started notifications indicates the connection is successful.



## Ingestion Node Notifications

The Ingestion Node also sends notifications for the following events:

- Node is registered - Ingestion Node is started
- EPD exceeds 80% of daily limit
- EPD exceeds 100% of daily limit
- EPD exceeds 120% of daily limit [Ingestion is suspended in this case!]
- Ingestion is resumed after suspension
- DU exceeds 50% of allocated disk space
- DU exceeds 75% of allocated disk space
- DU exceeds 90% of allocated disk space
- DU exceeds 95% of allocated disk space
- License expiry is less than or equal to 10 days - Ingestion Node is shutting down.

## Stopping the Ingestion Node

To stop the Ingestion Node service on the Ingestion Node server, use this command:

```
service scn-x-ingester stop
```

# Troubleshooting the Ingestion Node

This section highlights some common troubleshooting issues that may appear with the Ingestion Node on the ArcSight UBA Console.

## Ingestion Node Installation Issues

### *Creation of ingestercloud.properties fails during installation*

During installation, the installer attempts to connect to the ArcSight UBA Console web service to generate the required ingestercloud.properties file under the \$INGESTER\_HOME/conf folder, using the supplied URL, admin user and admin password. If the installer cannot reach the ArcSight UBA Console, or if there is an SSL trust issue due to the ArcSight UBA Console being deployed with SSL and using a self-signed certificate, this file needs to be manually generated. See [Appendix A](#) for the instructions to create this file.

## Ingestion Node Post Installation Issues

### *Authentication checks*

See [Appendix A](#) for the instructions to create the ingestercloud.properties file.

- Token validation fails
- URL or token is not provided in ingestercloud.properties file

### *Kafka publishing fails with SSL error*

- If the Kafka Brokers are protected with SSL and use self signed certificates, the truststore and SSL config file, sslconfig.properties, located in the \$INGESTER\_HOME/conf folder must be configured to point to the truststore.jks and the public keys of the Kafka brokers, or the public key of the signing certificate must be imported to the truststore.jks. See [Appendix A](#) for instructions.
- If the Kafka Brokers are configured with mutual SSL authentication, a client certificate must be imported into the keystore for the Ingester. The SSL config file sslconfig.properties, located in the \$INGESTER\_HOME/conf folder, must be configured to point to the ingester-client.jks. See [Appendix A](#) for instructions.

## Ingestion Node Log File for Troubleshooting

To troubleshoot or examine the Ingestion Node log file, use this command:

```
tail -1234f /<your_installation_path>/Ingester/service/scnx-ingester/scnx-ingester.log
```

Generally, the default log level is set to debug in the Ingestion Node log file. If you would like to define a custom log level, change the log4j2.xml log level to trace. The file is available at \$INGESTER\_HOME/conf/log4j2.xml.

## ArcSight UBA Console Issues

- Unable to initialize Web Service client
- Unable to obtain Hadoop configuration
- Unable to initialize Kafka producer



**Note:** During shutdown, Ingestion Node clears the properties files used by Syslog-ng service to filter and publish events. This is to ensure that no events are published once the Ingestion Node is shut down.

- Unable to obtain or register the Ingestion Node node (refers to the Ingester table)

# Uninstalling the Ingestion Node

To uninstall the Ingestion Node, complete the following steps:

1. Stop `scnx-syslog-ng`, `scnx-ingester`, and `scnx-arcsight_eb_to_securonix` services.

2. Delete the files using these commands as **securonix** user:

```
sudo rm -rf /etc/init.d/scnx-ingester
sudo rm -rf /etc/init.d/scnx-syslog-ng
sudo rm -rf /usr/bin/wmic
rm -rf /your_installation_path/
rm -rf /Securonix/syslog/
unset INGESTER_HOME
sudo rm -rf /etc/init.d/scnx-arcsight_eb_to_securonix
```

3. Open the file `/.bash_profile` using this command:

```
vi ~/.bash_profile
```

4. Delete the line **export INGESTER\_HOME = /your\_installation\_path/**.

# Appendix A - Configuring the Ingestion Node Properties Files

This appendix contains information about the properties files that are available with the Ingester, and the process to manually configure the properties in each file. The property files are configured during installation of the Ingestion Node. However, if there is an issue with the keystore, truststore or the network connectivity to the ArcSight UBA Console during the RIN installation, you may need to manually configure the files after installing the Ingestion Node.

## Step 1: Generating the ingestercloud.properties file



**Note:** Before you generate the ingestercloud.properties file, ensure that the ArcSight UBA Console is installed and running. Also, it should be accessible from the server where the RIN is installed.

Optional: Import the public key of the Console into the Java truststore. This step is required if the Console is configured with SSL, and is using a self-signed certificate.

1. Export the public key from the ArcSight UBA Console into the Java truststore. This is a required step if the ArcSight UBA Console is configured with SSL, and it is using a self-signed certificate.

```
/<Installation DIR>/Console/Java/jre/bin/keytool -export -
keystore /<Installation
DIR>/Console/Tomcat/conf/securonixKeyStore -alias
securonixSIEMKS -file consolepublic.cer
```

The names of the keystore and alias are the defaults created by the ArcSight UBA installer. If you prefer to use an alternate name, replace those values with your values.

2. Copy the public key of the ArcSight UBA Console to the Ingester server.
3. Import the public key into the Ingester truststore.

```
$INGESTER_HOME/Java/jre/bin/keytool -import -alias
securonixSIEMKS -file consolepublic.cer - keystore $INGESTER_
HOME/conf/truststore.jks
```

Use this command as a securonix (non-root) user on the Ingestion Node host to generate a token.

```
/ $INGESTER_HOME/Java/jre/bin/java -jar $INGESTER_
HOME/Utilities/TokenGenerator-1.0.jar -url: <http
(s)://fqdn:port/Snypr> -
username:admin -password:<password> -tenant:<tenantid>
```

A new ingestercloud.properties file will be generated. For example:

```
Generating token ..
Token:<tokened>
File: <APTH>/RIN/conf/ingestercloud.properties
Done!
```



*Timers Available in the Ingestion Node Cloud Properties File*

- COUNT TIMER - If EPD interval is provided, the timer periodically validates published counts against EPD. The timer is set at 10 seconds.
- EPD UPDATE TIMER - If EPD interval is provided, epd.update.interval periodically gets published counts from the ArcSight UBA Console and updates the Ingestion Node. This property also performs validation.
- DU UPDATE TIMER - The diskusage.update.interval timer gets disk usage from the console and validates against the allocated/licensed disk space.
- CONFIG UPDATE TIMER - The config.update.interval periodically gets the control flags from the ArcSight UBA console. The control flags are set in Console when:
  - Resource group is created, updated or deleted
  - AD user import is configured
  - License is installed or uninstalled
  - Job schedule is updated
  - Preview is requested for activity or user data

## Step 2: Configuring the SSL Keystores and Properties Files

The sslconfig.properties file contains the SSL settings. The Ingestion Node reads the SSL properties from the sslconfig.properties file if SSL is enabled for Kafka. The keystore and truststore need to be configured if self-signed certificates are used.



**Note:** These values are needed only if SSL is enabled for the Kafka brokers.

### Import the Public Key of the Kafka Brokers into the Truststore

This step is required if the Kafka brokers are configured with SSL and are using self-signed certificates.

1. Export the public key from the Kafka Brokers keystore



**Note:** Perform this step for each of the Kafka brokers if they are not using a signing certificate to establish a trust chain. If a signing certificate is used, export the public key from the signing certificate only.

```
keytool -export -keystore <keystore> -alias <alias> -file
brokerpublic.cer
```

2. Import the public key into the Ingestion truststore.

```
keytool -import -alias broker -file brokerpublic.cer -keystore
$INGESTER_HOME/conf/truststore.jks
```

## Import the Private Key of the RIN into the Keystore

This step is required if the Kafka brokers are configured with SSL and mutual authentication with client certificates on the RIN.

1. Copy the Ingestion Node public key to the Ingester server.



**Note:** This can be a self-signed certificate or a production certificate. If this is a self-signed certificate, it is recommended that this certificate be signed by a Certificate Authority (CA) that also signed the Kafka broker certificates.

2. Import the public key into the Ingester truststore.

```
keytool -importkeystore -noprompt -deststorepass <TSPASSWORD> -
destkeypass <KPASSWORD> -destkeystore <INGESTER_
HOME>/conf/ingester-client.jks -srckeystore <rincert>.p12 -
srcstoretype PKCS12 -srcstorepass <TKPASSWORD> -alias <tenantid>
```

- Generate the hashed password for the truststore, keystore, and client certificate for inclusion in the sslconfig.properties.

From your keyboard:

```
cd <$INGESTER_HOME>/lib
```

- Generate the value for truststore.password.



**Note:** Replace the password with the actual truststore password.

```
java -cp securonixlib-1.1.jar:log4j-1.2.17.jar
com.securonix.lib.EDUtil -e '<truststore-password>'
Output: B0C7F0D0DAD0E99D6CB79C872C5C98CD
```

Repeat the step for the truststore.password, the keystore.password, and the key.password.

- Edit the sslconfig.properties for the Ingester:

```
cd <$INGESTER_HOME>/conf/
vi sslconfig.properties
```

The sslconfig.properties file may include a hashed password for the following key value pairs. Replace the **<hashed password>** with the generated hash from the previous commands for each key value:

```
truststore.location=${INGESTER_HOME}/conf/ingester/client.truststore.jks
truststore.password=<hashed password>
keystore.location=${INGESTER_HOME}/conf/ingester/client.keystore.jks
keystore.password=<hashed password>
key.password=<hashed password>
```

- Save and exit the sslconfig.properties file using the following command:

```
:wq
```

## Step 3: Verify the Remote `ingestercloud.properties` File

The `ingestercloud.properties` file contains the properties for the Ingestion Node as follows:

- `url`: to access ArcSight UBA web service
- `token`: for accessing the web service (without IP validation)
- `node.name`: unique identifier for the node
- `config.update.interval`: interval at which the Ingestion Node will check for control flags
- `epd.update.interval`: interval at which the Ingestion Node will get published count from the console and perform validation (upper limit is 1 hour)
- `diskusage.update.interval`: interval at which the Ingestion Node will get disk usage details from the console and perform validation. The default interval is at 30 seconds. The disk usage is based on the licensing options.

All intervals are in seconds. You must either specify Events Per Day (EPD) or Disk Usage (DU) interval.

The following HTTP fields within the Ingestion Node are for future use.

- `http.server.enabled`
- `http.server.port`
- `http.server.contextUrl`

### Timers Available in the `ingestercloud.properties` File

- **COUNT TIMER** - If EPD interval is provided, the timer periodically validates published counts against EPD. The timer is set at 10 seconds.
- **EPD UPDATE TIMER** - If EPD interval is provided, `epd.update.interval` periodically gets published counts from the Console and updates the Ingestion Node. This property also performs validation.
- **DU UPDATE TIMER** - The `diskusage.update.interval` timer gets disk usage from the console and validates against the allocated/licensed disk space.
- **CONFIG UPDATE TIMER** - The `config.update.interval` periodically gets the control flags from the Console. The control flags are set in Console when:
  - Resource group is created, updated or deleted
  - AD user import is configured
  - License is installed or uninstalled
  - Job schedule is updated
  - Preview is requested for activity or user data

# Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

**Feedback on Documentation (Micro Focus ArcSight User Behavior Analytics 6.10)**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to [arst-techpubs@hpe.com](mailto:arst-techpubs@hpe.com).

We appreciate your feedback!