Red Hat Insights 2021

Configuring Basic Authentication for Red Hat Insights

Last Updated: 2021-09-13

Legal Notice

Abstract

Configure basic authentication in order to use Insights for Red Hat Enterprise Linux on Red Hat Enterprise Linux (RHEL) systems managed by Red Hat Update Infrastructure (RHUI).

Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see our CTO Chris Wright's message.

PROVIDING FEEDBACK ON RED HAT HYBRID CLOUD CONSOLE DOCUMENTATION

We appreciate your input on our documentation. Please let us know how we could make it better. To do so, create a Bugzilla ticket:

1. Go to the Bugzilla website.
2. As the Component, use **Documentation**.
3. Fill in the **Description** field with your suggestion for improvement. Include a link to the relevant part(s) of documentation.
4. Click **Submit Bug**.

CHAPTER 1. BASIC AUTHENTICATION OVERVIEW

Insights for Red Hat Enterprise Linux can use two types of authentication to validate system access to the Insights for RHEL services. The default authentication method is through certificates. Certificates are generated when you register a system with Red Hat Subscription Manager (RHSM) or when your system is managed by Red Hat Network Satellite system management.

An alternative authentication method is through SSO credentials. A valid Red Hat SSO credential is created when you have a valid Red Hat Customer Portal user name. In order to use SSO credentials with Insights for Red Hat Enterprise Linux, you must configure your system to use basic authentication.

1.1. WHEN TO USE BASIC AUTHENTICATION

You must use basic authentication in any of the following situations:

- Your RHEL system is not registered with Red Hat Subscription Manager (RHSM).
- Your Red Hat Enterprise Linux (RHEL) system is not managed by Red Hat Network Satellite services.
- Your RHEL system is provisioned through a Red Hat Certified Cloud and Service Provider and is updated by Red Hat Update Infrastructure (RHUI).
- Your RHEL system is from a cloud marketplace provider and not obtained through Red Hat Cloud Access program.

NOTE

If you have valid RHEL subscriptions for your system, you can switch between the default certificate-based authentication for Insights for RHEL and the basic authentication for Insights for RHEL. If you are configuring basic authentication on a new RHEL system, you must complete the basic authentication procedures before you can register the Insights for RHEL client application.

1.2. CONFIGURATION REQUIREMENTS FOR BASIC AUTHENTICATION

When you configure your system to use single sign-on (SSO) credentials for basic authentication instead of the default certificate-based authentication for Insights for Red Hat Enterprise Linux, you provide Red Hat SSO credentials. SSO credentials are a valid Red Hat Customer Portal user name and password.

To configure basic authentication, a plain-text username and password is stored in the configuration file. As a best practice, create a Red Hat Customer Portal account with SSO credentials that are used only for Insights for Red Hat Enterprise Linux basic authentication. This action avoids exposing the SSO credentials of individual users.

1.3. HOW TO KNOW IF YOU MUST CONFIGURE BASIC AUTHENTICATION

The following messages might appear when you attempt to register a system that does not have a Red Hat authentication certificate. If you see **=== End Upload URL Connection Test: FAILURE ===**, configure your system for basic authentication.

```
insights-client --register
Running connection test...
Connection test config:
=== Begin Certificate Chain Test ===
depth=1
verify error:num=0
verify return:1
depth=0
verify error:num=0
verify return:1
=== End Certificate Chain Test: SUCCESS ===

=== Begin Upload URL Connection Test ===
HTTP Status Code: 401
HTTP Status Text: Unauthorized
HTTP Response Text:
Connection failed
=== End Upload URL Connection Test: FAILURE ===

=== Begin API URL Connection Test ===
HTTP Status Code: 200
HTTP Status Text: OK
HTTP Response Text: lub-dub
Successfully connected to: https://cert-api.access.redhat.com/r/insights/
=== End API URL Connection Test: SUCCESS ===

Connectivity tests completed with some errors
See /var/log/insights-client/insights-client.log for more details.
```

CHAPTER 2. CONFIGURING BASIC AUTHENTICATION

Insights client configuration is managed in **/etc/insights-client/insights-client.conf**. This file provides a configuration template for setting up basic authentication. The default configuration for certificate-based authentication is as follows:

```
auto_config=TRUE
authmethod=BASIC
username=<your customer portal username>
password=<your customer portal password>
```

Prerequisites

- You have a Red Hat SSO username and SSO password that can be stored in clear text.
- You have read/write permissions in the directory **/etc/insights-client/**.
- The **insights-client** package is installed on your system.

Procedure

1. Use a text editor to open the file **/etc/insights-client/insights-client.conf**
2. Change **auto_config=TRUE** value to **auto_config=FALSE**.
3. Replace **<your customer portal username>** with a Red Hat SSO username.
4. Replace **<your customer portal password>** with a Red Hat SSO password.
5. Save the configuration and exit the editor.
6. Register the system.

```
# insights-client --register
```