

USER GUIDE

HYCU SCOM Management Pack for F5 BIG-IP

Version: 5.8.2
October 2022



Legal notices

Copyright notice

© 2022 HYCU. All rights reserved.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, distributed, transmitted, stored in a retrieval system, modified or translated to another language in any form by any means, without the prior written consent of HYCU.

Trademarks

HYCU logos, names, trademarks and/or service marks and combinations thereof are the property of HYCU or its affiliates. Other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at [f5.com](https://www.f5.com). Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5.

Microsoft and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Disclaimer

The details and descriptions contained in this document are believed to have been accurate and up to date at the time the document was written. The information contained in this document is subject to change without notice.

HYCU provides this material "as is" and makes no warranty of any kind, expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. HYCU shall not be liable for errors and omissions contained herein. In no event shall HYCU be liable for any direct, indirect, consequential, punitive, special or incidental damages, including, without limitation, damages for loss and profits, loss of anticipated savings, business interruption, or loss of information arising out of the use or inability to use this document, or any action taken based on the information contained herein, even if it has been advised of the possibility of such damages, whether based on warranty, contract, or any other legal theory.

The only warranties for HYCU 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.

Notice

This document is provided in connection with HYCU products. HYCU may have copyright, patents, patent applications, trademark, or other intellectual property rights covering the subject matter of this document.

Except as expressly provided in any written license agreement from HYCU, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property on HYCU products. Use of underlying HYCU product(s) is governed by their respective Software License and Support Terms.

Important: Please read Software License and Support Terms before using the accompanying software product(s).

HYCU

www.hycu.com

Contents

Environment preparation	8
Installation prerequisites	8
Configuring SNMP access to BIG-IP devices	9
Configuring F5 BIG-IP iControl REST API access	10
Process overview	10
Verifying BIG-IP device access	11
Configuring monitoring user accounts	11
Creating SCOM resource pools	16
Discovering BIG-IP devices as network devices in SCOM	16
Installation and configuration	18
Obtaining the product installation package	18
Installing the product	18
Configuring HYCU F5 BIG-IP Device Action Account with SCOM Operations console	25
Configuring HYCU F5 BIG-IP default port	27
Setting up Data Warehouse Action Account for F5 BIG-IP devices	27
Compliance with Federal Information Processing Standards (FIPS)	28
Upgrade	29
Product licensing	30
Prerequisites for licensing tasks	30
Activating software evaluation and universal licenses	30
Activating perpetual (permanent) licenses	31
Generating license request files for all unlicensed devices	31
Generating license request files for individual devices	32
Applying license activation files	32
Functionality overview	34
General product functionality	34
Alerts	34

All Performance Graphs	34
MP Administration	34
HYCU Management Pack for F5 BIG-IP Device (Core)	34
Device performance views	35
Device Diagram	35
Hardware Alerts	35
HYCU Management Pack for F5 BIG-IP Device (Reports)	35
HYCU Management Pack for F5 BIG-IP LTM (Core)	36
Dashboards	36
LTM performance views	37
LTM Diagram	37
Filtering virtual servers, pools, and pool members	37
HA monitoring	38
HYCU Management Pack for F5 BIG-IP LTM (Reports)	39
HYCU Management Pack for F5 BIG-IP ASM (Core)	39
ASM Statistics Dashboard	39
ASM Security Policies	40
HYCU Management Pack for F5 BIG-IP ASM (Reports)	40
HYCU Management Pack for F5 BIG-IP DNS (Core)	40
Some of the F5 BIG-IP Devices in F5 DNS Sync Group are not in sync monitor	40
DNS Wide IP Performance view	41
Wide IPs view	41
Filtering DNS objects	41
BIG-IP objects, properties, and relationships	42
Uninstallation	44
Uninstallation overview	44
Removing included management packs	44
Uninstalling SCOM MP for F5 BIG-IP from management server	45
Troubleshooting	46
General troubleshooting guidelines	46

Problems and solutions	46
Registry key access failure during product upgrade	46
REST query to a BIG-IP device results in an error	47
BIG-IP devices are not discovered	47
Workflows are not triggered	50
Alerts are not generated or performance data is not collected	51
ASM Statistics Dashboard is not available in the SCOM web console	51
ASM Statistics Dashboard is empty	51
Some virtual servers are missing in ASM Statistics Dashboard	52
Self IP Address property is empty	52
Rest Framework Version and Is Virtual properties are empty	53
Health recalculation does not change the monitor's health indicator	53
Getting assistance	54
Licensing assistance	54
Support	54
Getting additional information and latest updates	55
Before contacting HYCU Customer Support	55
Advanced tasks	57
Installing the product in quiet mode or passive mode	57
Quiet installation	57
Passive installation	58
Upgrading the product from a version earlier than 3.0	58
Manually importing included management packs	59
Creating a management pack for overrides	60
Putting BIG-IP devices into maintenance mode	60
Configuring HYCU F5 BIG-IP Device Action Account with Windows PowerShell	61
Distributing Run As accounts to all SCOM management servers	62
Distributing Run As accounts to a specific SCOM resource pool	62
Verifying Run As accounts	63
Advanced script usage	63
Adjusting SCOM configuration for large environments	66
HYCU Customer Support and information	69

Customer Support	69
Company website and video channel	69
General information	70
Feedback	70

Chapter 1

Environment preparation

This chapter contains instructions for preparing your environment for installation of HYCU SCOM Management Pack for F5 BIG-IP.

Installation prerequisites

Before installing HYCU SCOM Management Pack for F5 BIG-IP (SCOM MP for F5 BIG-IP), make sure that the following prerequisites are fulfilled:

- Versions of the following products that you are using are compatible with SCOM MP for F5 BIG-IP:

- F5 BIG-IP devices
- System Center Operations Manager

For a list of the supported versions, see the HYCU SCOM Management Pack for F5 BIG-IP Compatibility Matrix

- **F5 BIG-IP infrastructure prerequisites:**

- Your F5 BIG-IP devices are accessible.

For instructions on how to configure proper access to the BIG-IP devices, see sections [“Configuring SNMP access to BIG-IP devices” on the next page](#) and [“Configuring F5 BIG-IP iControl REST API access” on page 10](#).

- **System Center Operations Manager (SCOM) platform prerequisites:**

- Each of the SCOM management servers can access BIG-IP devices through standard ports of the protocols used:
 - SNMP: port 161 (UDP)
 - HTTPS:
 - port 443 (TCP): default port for device management with multiple network interfaces, or
 - port 8443 (TCP): default port for device management with single network interface, or
 - custom port for device management, depending on the BIG-IP device configuration.

Optional. Each of the SCOM gateway servers can communicate with the SCOM management servers through the standard SCOM interconnection port 5723 (TCP).

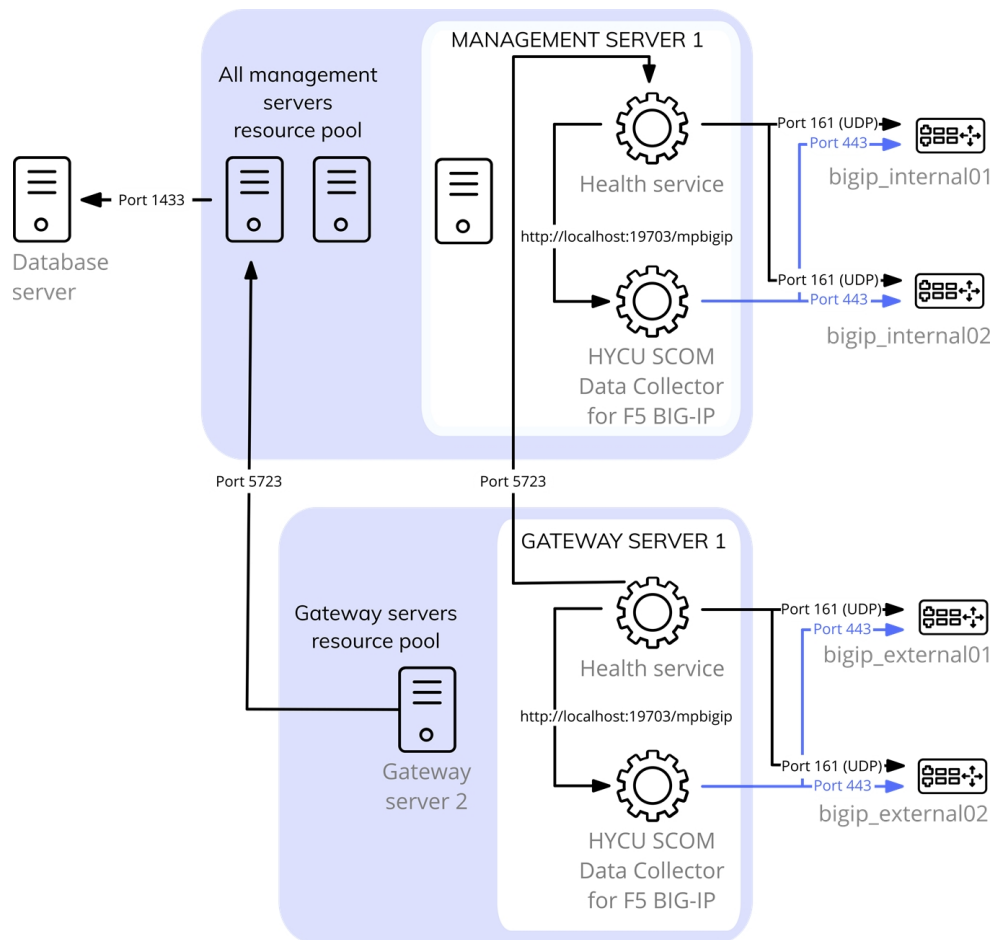


Figure 1-1: A SCOM deployment for BIG-IP device monitoring that includes gateway servers

- A SCOM resource pool dedicated to monitoring BIG-IP devices exists.
For instructions on how to create an appropriate SCOM resource pool, see section [“Creating SCOM resource pools”](#) on page 16.
- BIG-IP devices are visible to SCOM as network devices.
For instructions on how to discover BIG-IP devices as network devices in SCOM, see section [“Discovering BIG-IP devices as network devices in SCOM”](#) on page 16.

Configuring SNMP access to BIG-IP devices

For each BIG-IP device that you plan to monitor, you must ensure that the device is accessible by SCOM through both SNMP (Internet Standard protocol) and iControl REST API (F5 proprietary interface). This section guides you through the SNMP access configuration.

You should complete the below procedure for each BIG-IP device that you plan to monitor.

To configure SNMP access to an F5 BIG-IP device, do the following:

1. Log on to the BIG-IP Traffic Management Shell (tmsh) with administrator credentials.
2. In tmsh, to add a SCOM management server as an SNMP agent, run the following command:

```
modify sys snmp allowed-addresses add { <IPaddress> }
```

In this instance, *<IPaddress>* is the IP address of the SCOM management server from the SCOM resource pool that should be used to monitor BIG-IP devices.

Example

```
modify sys snmp allowed-addresses add { 10.81.9.67 }
```

3. Check if an SNMP community string is added on the BIG-IP device. If the community string is missing, to add it, run the following command:

```
modify sys snmp communities add { test_community { community-name "<CommunityString>" source "<IPaddress>" } }
```

In this instance, *<CommunityString>* is the community string that should be used when discovering these BIG-IP devices in SCOM. *<IPaddress>* is the IP address of the SCOM management server.

Example

```
modify sys snmp communities add { test_community { community-name "test" source "10.81.9.67" } }
```

4. Repeat step 3 for each additional SCOM management server from the SCOM resource pool that you plan to use for monitoring BIG-IP devices.
5. To save configuration changes, run the following command:

```
save sys config
```

Configuring F5 BIG-IP iControl REST API access

For each BIG-IP device that you plan to monitor, you must ensure that the device is accessible by SCOM through both SNMP (Internet Standard protocol) and iControl REST API (F5 proprietary interface). This section guides you through the configuration of iControl REST API access.

Process overview

The process for enabling monitoring of a F5 BIG-IP device through its iControl REST API consists of the following tasks:

1. Verify accessibility of a device from a SCOM management server.
2. On a BIG-IP device, configure a user account dedicated to device monitoring (referred to as *monitoring user account*).

You should complete the above process for *each* BIG-IP device that you plan to monitor and for *each* SCOM management server that you plan to use.

Verifying BIG-IP device access

To check if the F5 BIG-IP iControl REST service on a BIG-IP device is accessible by using the HTTPS protocol, complete the verification procedure that follows.

Verification

Do the following:

1. On a SCOM management server that you plan to use for monitoring, open a web browser, and go to the following webpage:


```
https://<IPaddress>:<port>
```


In this instance, *<IPaddress>* is the IP address of the chosen BIG-IP device and *<port>* is the port for device management.

2. Check if the BIG-IP Configuration Utility (web user interface) opens in the web browser.

Configuring monitoring user accounts

Monitoring user account can be either local BIG-IP user or remote depending on whether BIG-IP is configured to use local or remote authentication (e.g. authentication with remote Active Directory)

 **Note** If you choose remote authentication, make sure that the remote user account is not part of a BIG-IP remote role group.

 **Important** Read through this section before you start configuring your monitoring user account, to see which user account roles and which access authentication methods are available.

Monitoring user account roles

You can use a user account with any role except "No Access" can be used.

If you choose a user role other than Administrator, additional steps must be followed to enable read-only access to IControl REST API for the selected user account as documented in ["Configuring monitoring user accounts for F5 BIG-IP" on the next page](#).

Access authentication methods

Independently of the configured user account types, BIG-IP devices support two access authentication methods:


- Standard HTTP authentication

This method is also referred to as *basic access authentication*. It is available in all F5 BIG-IP versions.

- F5 proprietary token scheme

This method, also referred to as *token-based authentication*, is more secure than basic access authentication. In addition, it reduces authentication traffic on BIG-IP devices, resulting in greater responsiveness of the devices.

This method is available in the F5 BIG-IP versions 12.0 and later.

 **Important** SCOM MP for F5 BIG-IP automatically uses token-based authentication with all F5 BIG-IP versions that support this access authentication method.

Configuring monitoring user accounts for F5 BIG-IP

There are two ways to complete the configuration process. For configuration, you can use:

- BIG-IP Configuration Utility (graphical user interface)

See [“Configuration Utility-based configuration procedure”](#) below.

- BIG-IP Traffic Management Shell (command-line interface)

See [“Traffic Management Shell-based configuration procedure”](#) on the next page.

Configuration Utility-based configuration procedure

To configure a monitoring user account by using the BIG-IP Configuration Utility, do the following:

1. Open a web browser and log in to the BIG-IP Configuration Utility with a user account that has privileges to create BIG-IP user accounts.
2. Navigate to **System > Users > User List**.
3. Click **Create**.
4. Depending on whether BIG-IP device uses remote or local authentication specify user
 - Local authentication
 - Enter a value for the Account User Name option.
 - Enter the password that you want to use for this user account.
 - Remote authentication
 - In the Account User Name text box, enter the user name of the monitoring

account that was created in the remote authentication system (for example, Active Directory).

Example

Value of the Account User Name option in BIG-IP:

```
MyMonitoringAccountName
```

5. Assign the user account a user role and partition access:

You can choose any role except No Access. For a user account that is assigned a user role other than Administrator, you must follow additional steps.

For partition access, select All.

Example

Assigned BIG-IP user role:

```
Guest
```

6. Click **Finished**.
7. *Mandatory if you are setting up a user account with a non-administrative role.*

On a SCOM management server that can access the BIG-IP device, run the following Windows PowerShell script to enable read only access to iControl TEST API on BIG-IP device for the monitoring user:

```
Set-ReadOnlyAccess.ps1
```

The script is located in the Program Files directory (default location: C:\Program Files (x86)\Comtrade Software\HYCU SCOM MP for F5 BIG-IP\Management packs\Configuration tools).

In PowerShell enter the following command: `.\Set-ReadOnlyAccess.ps1`

8. *Mandatory if you are setting up a user account with a non-administrative role.*

When prompted, enter the following information:

- IP address of the BIG-IP device on which you created the user account
- User name of the created user account
- Credentials of a user account that has administrative privileges in BIG-IP

To verify your monitoring user account configuration, see part *Verification* at the end of the next section.

Traffic Management Shell-based configuration procedure

To configure a monitoring user account by using the BIG-IP Traffic Management Shell, do the following:

1. Log on to the BIG-IP Traffic Management Shell (tmsh) with a user account that has privileges to create BIG-IP user accounts.

2. Action in this step depends on the chosen user account type:

- Remote user account:

In tmsh, run the following command:

```
create auth user <HYCUf5BIGipMonitoringAccount> partition-access
add { all-partitions { role <MyRole> } } shell none
```

In this instance, *<HYCUf5BIGipMonitoringAccount>* is the user name of the user account.

<MyRole> can be any role except No Access. For a user account that is assigned a user role other than Administrator, you must follow additional steps.

- Local user account:

In tmsh, run the following command:

```
create auth user <HYCUf5BIGipMonitoringAccount> password
<MyPassword> partition-access add { all-partitions { role <MyRole>
} } shell none
```

In this instance, *<HYCUf5BIGipMonitoringAccount>* is the user name of the user account, *<MyPassword>* is the password that you want to use for this user account.

<MyRole> can be any role except No Access. or a user account that is assigned a user role other than Administrator, you must follow additional steps.

3. To verify that the user account is created, run the following command:

```
list auth user
```

The command output should resemble the example output that follows.

Example

Command output for local user account:

```
auth user MyMonitoringAccountName {
  description MyMonitoringAccountName
  encrypted-password
"$6$gj09Xaj/$P2TkRsh4r2sdVbsdutM.FoeWPjk8gdJIIyPdhD/cV/vG5kqSL9LWvAUS
.l.iAf7j8WmB61kKi8infxID1Y7CFEaX30"
  partition Common
  partition-access all
  role admin
  shell none
}
```

4. To save system configuration, run the following command:

```
save sys config
```

5. *Mandatory if you are setting up a user account with a non-administrative role.*

On a SCOM management server that can access the BIG-IP device, run the following Windows PowerShell script to enable read only access to iControl REST API on BIG-IP device for the monitoring user:

```
Set-ReadOnlyAccess.ps1
```

The script is located in the Program Files directory (default location C:\Program Files (x86)\Comtrade Software\HYCU SCOM MP for F5 BIG-IP\Management packs\Configuration tools).

In PowerShell enter the following command: `.\Set-ReadOnlyAccess.ps1`

6. *Mandatory if you are setting up a user account with a non-administrative role.*

When prompted, enter the following information:

- IP address of the BIG-IP device on which you created the user account
- User name of the created user account
- Credentials of a user account that has administrative privileges in BIG-IP

Verification

This verification step checks whether BIG-IP device can be accessed from SCOM management server with monitoring account. Verification steps depend on the access authentication mode used by SCOM MP for F5 BIG-IP.

Do the following:

1. On a SCOM management server that can access the BIG-IP device, run the following Windows PowerShell script:

```
Verify-TokenAccess.ps1 -Devices <IPAddress>
```

In this instance, `<IPAddress>` is the IP address of the BIG-IP device for which you want to verify access to the iControl REST API. For verifying multiple BIG-IP devices at once, list all devices separated by “,”.

Example usage: `Verify-TokenAccess.ps1 -Devices 10.49.0.1,10.49.0.2,10.49.0.3`

When prompted, provide the credentials of a user account that has administrative privileges in BIG-IP.

The script is located in the Program Files directory (default location: C:\Program Files (x86)\Comtrade Software\HYCU SCOM MP for F5 BIG-IP\Management packs\Configuration tools).

2. Check if the script output resembles the following:

```
StatusCode StatusDescription
-----
200 OK
```

Creating SCOM resource pools

To achieve high availability monitoring of BIG-IP devices, you should have a SCOM resource pool with at least two dedicated SCOM management servers.

To create a SCOM resource pool for monitoring BIG-IP devices, do the following:

1. In the SCOM Operations console, navigate to **Administration > Resource Pools**.
2. Right-click the pane that appears and click **Create Resource Pool**.
3. Enter a name for this SCOM resource pool (for example, BIG-IP Resource Pool or F5 Resource Pool), and then click **Next**.
4. Click **Add** and then click **Search**.
5. Select SCOM management servers that you wish to add to this SCOM resource pool, and then click **Add**.
6. Once you have added all designated SCOM management servers, click **OK**.
7. Click **Next**.
8. Click **Create**.

Verification

Do the following:

1. In the SCOM Operations console, in the **Administration** view, click **Resource Pools**.
2. Check if the name of the created SCOM resource pool is present in the Resource Pools list.

Discovering BIG-IP devices as network devices in SCOM

As a prerequisite for SCOM MP for F5 BIG-IP, all F5 BIG-IP devices must be discovered and monitored as network devices by SCOM.


To achieve monitoring of BIG-IP devices in Sync-Failover device group, all devices from Sync-Failover device group must be discovered with the same Network Devices Discovery.

The following is an example scenario for discovering BIG-IP devices in the System Center Operations Manager.

To discover BIG-IP devices as network devices in SCOM, do the following:

1. Launch the SCOM Operations console and connect to the management server.
2. Navigate to **Administration > Network Management > Discovery Rules** and invoke the **Discover Network Devices** task. The Network Devices Discovery wizard for creation of a discovery rule starts.

3. In the General Properties page, specify a discovery name, and choose a SCOM management server (**Available servers**) and a SCOM resource pool (**Available pools**, user-created) to be used for the discovery. Click **Next**.
4. In the Discovery Method page, select the discovery type, for example, **Explicit discovery**. Click **Next**.
5. In the Default Accounts page, click **Create Account** to create an SNMP Run As account. In the Create Run As Account Wizard window, enter the community string for **SNMP v1, v2** or account credentials for **SNMP v3** that are set in BIG-IP. Click **Create**. In the Network Devices Discovery Wizard window, click **Next**.
6. In the Device page, add each BIG-IP device that should be monitored and associate it with the SNMP Run As account created in the previous step. For the SNMP version option, select, for example, **v1, v2** or **v3**.
7. In the Schedule Discovery page, set the time to run the discovery rule or choose that the rule should be invoked manually. Click **Next**.
8. In the Summary page, verify your settings, and then click **Create**.
9. In the Warning dialog box, confirm account distribution by clicking **Yes**.

 **Tip** In case of issues with configuring network device discovery, follow general guidelines for network devices discovery in System Center Operations Manager. For more information, see the [How to Discover Network Devices in Operations Manager](#) webpage.

Verification

Do the following:

1. Keep the SCOM Operations console open and wait for the discovery process to complete.
2. Check if the fully qualified domain names of all BIG-IP devices are visible in the Network Devices list.
3. In the **Administration** view, expand **Network Management > Network Devices**.
4. Check if the fully qualified domain names of all BIG-IP devices are present in the Network Devices list.

Chapter 2

Installation and configuration

This chapter contains instructions for installing, verifying the installation of, and configuring HYCU SCOM Management Pack for F5 BIG-IP (SCOM MP for F5 BIG-IP).

Obtaining the product installation package

If you purchased a product license, go to the [F5 Monitoring – HYCU](#) webpage and sign in with your account credentials. If you do not have an account yet, apply for it at the support@hycu.com email address.

For instructions on how to upgrade from an earlier product version, see section [“Upgrading the product from a version earlier than 3.0” on page 58](#).

For instructions on how to adjust configuration of System Center Operations Manager and enable it to monitor large environments, see section [“Adjusting SCOM configuration for large environments” on page 66](#).

This product complies with the FIPS 140-2 standard. For more information, see section [“Compliance with Federal Information Processing Standards \(FIPS\)” on page 28](#).

Installing the product

HYCU SCOM Management Pack for F5 BIG-IP (SCOM MP for F5 BIG-IP) product consists of the following components:

- Management packs
- Data Collector (when selected in Setup Wizard)

This component is a Windows service that provides data caching and serves as a proxy between BIG-IP devices and SCOM MP for F5 BIG-IP. It listens for HTTP requests from SCOM MP for F5 BIG-IP and communicates with BIG-IP devices to collect their configuration and health statuses. The service uses port 19703 as the default local communication port on the SCOM management server. You can change the port number in the Setup Wizard before product installation starts.

- Other components (always installed)
 - Support tool
 - Licensing module

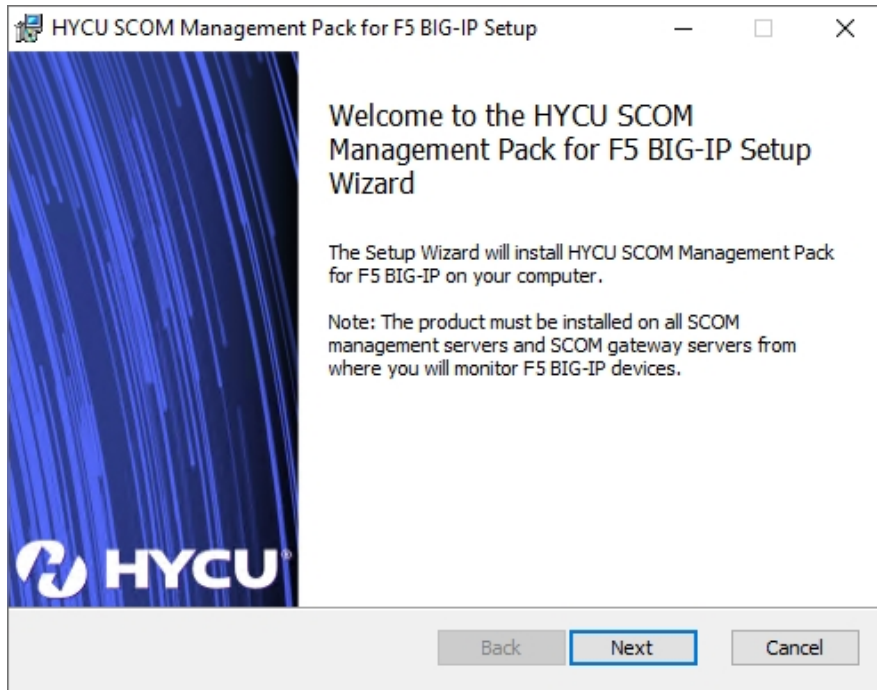
- Legal documents
- Documentation

 **Tip** You can also install SCOM MP for F5 BIG-IP in quiet mode or passive mode. For instructions, see section “Installing the product in quiet mode or passive mode” on page 57.

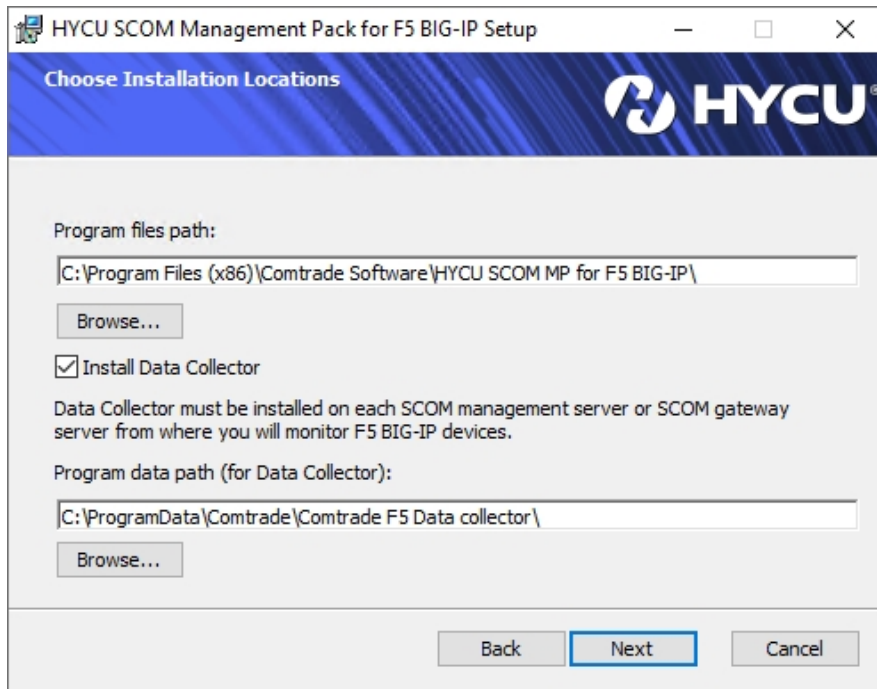
To install SCOM MP for F5 BIG-IP by using the Setup Wizard, do the following:

1. Go to the [F5 Monitoring - HYCU](#) webpage and sign in with your account credentials.
If you do not have an account yet, apply for it at the following email address:
support@hycu.com
2. When you are signed in, under Product download, click **HYCU SCOM Management Pack for F5 BIG-IP**.
3. Read through the Software License and Support Terms text. If you agree with the terms, click **Accept** and proceed.
4. In the Product download link line, click **Download** to transfer the product release archive and save it on the local system. Perform the steps that follow for each SCOM management server.
5. Copy the product release archive to the SCOM management server.
6. Log on to the SCOM management server with a user account that is assigned the Operations Manager Administrators user role.
7. In Windows Explorer, locate the `HYCU.SCOP.MP.F5.BIG-IP.<Version>.zip` file and extract its contents.
8. Locate the extracted `HYCU.SCOP.MP.F5.BIG-IP.msi` file and double-click it. The Setup Wizard starts.

- In the welcome screen, click **Next**.



- In the Choose Installation Locations screen, customize the installation locations if required and decide if you want to install Data Collector.



If you want to install the product to non-default location enter or select custom location in **Program files** path.

Data Collector must be installed on all SCOM management servers and SCOM gateway servers from where F5 BIG-IP devices will be monitored.

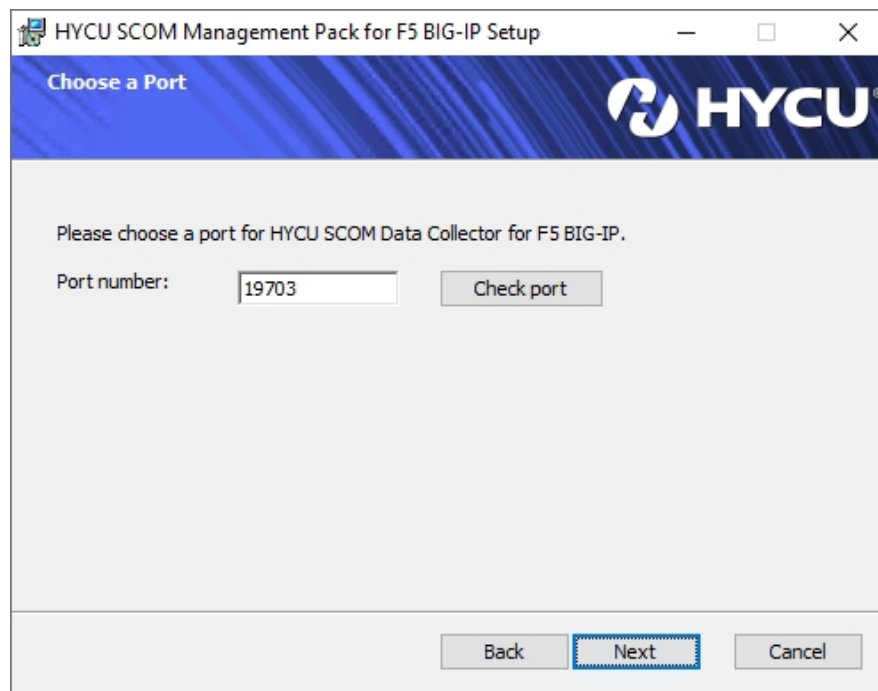
Note Data Collector should not be installed on SCOM management servers of SCOM deployments in which only SCOM gateway servers are used for monitoring of the devices.

The management packs must be imported only on one SCOM management server from the management group.

If Data Collector is selected for installation and you want to override default location for Data Collector runtime files, enter or select custom location in **Program data path (for Data Collector)**.

When finished, click **Next**.

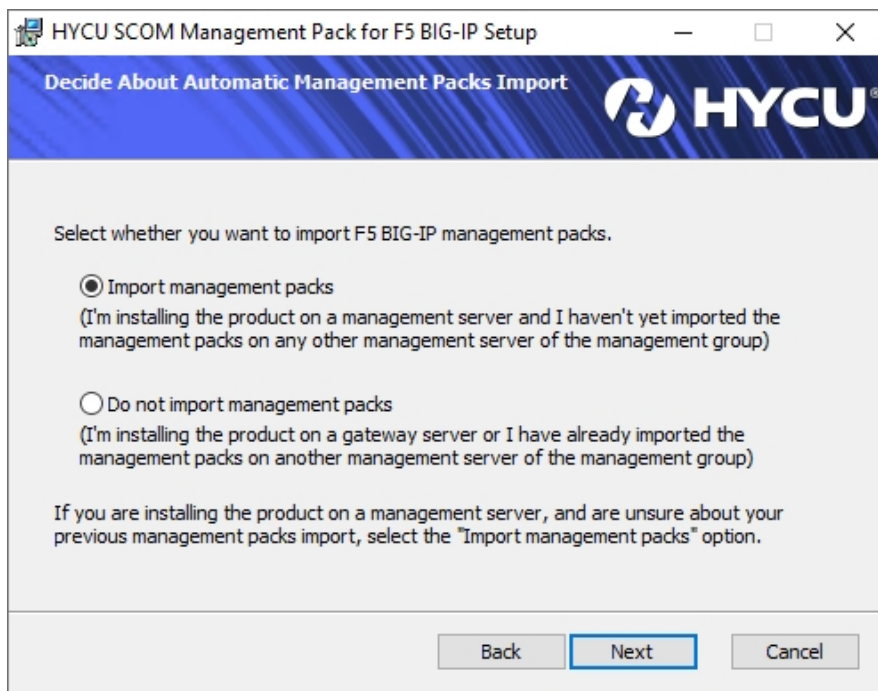
11. When Data Collector is selected for installation, the Choose a Port screen is displayed. Specify a free port number that the Data Collector should use for listening to management pack requests.



In the **Port number** text box, type the chosen port number and click **Check port** to verify its availability, if the port is already in use, and error message is reported, and you must specify a different port number.

When finished, click **Next**.

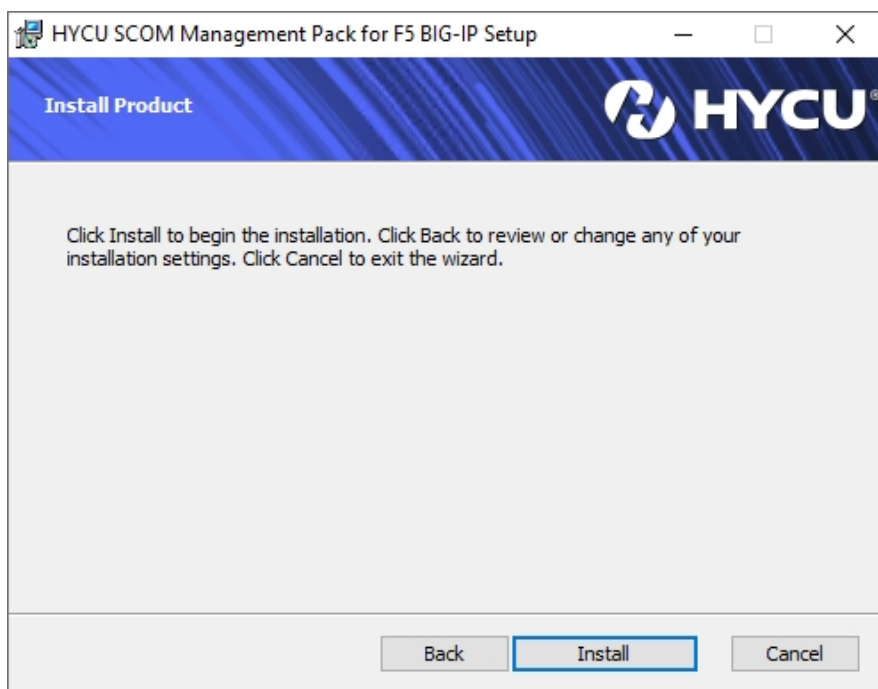
12. In this screen you decide if you want the Setup Wizard to automatically import the management packs.



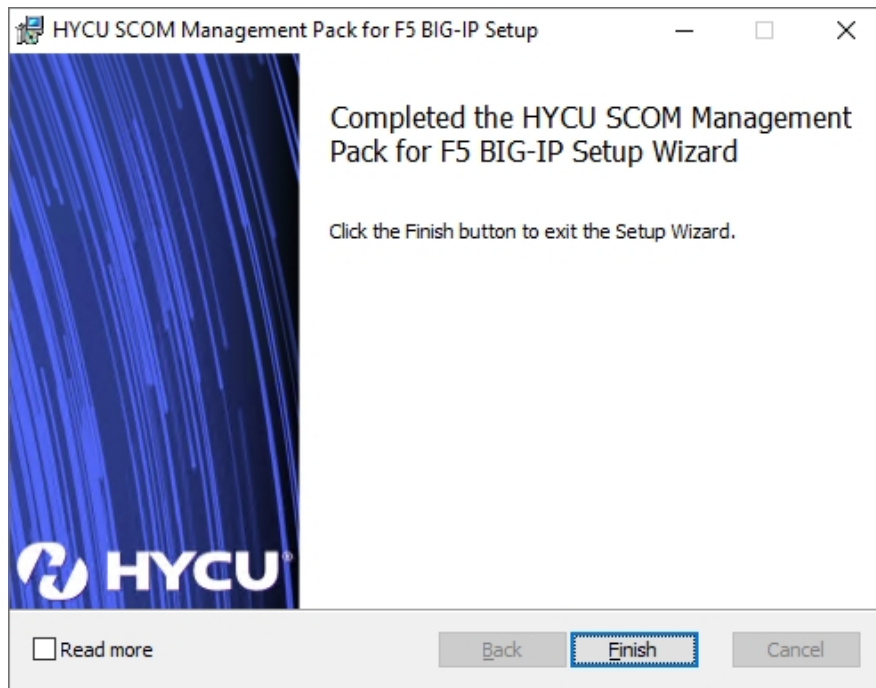
Follow instructions in the page, and keep the **Import management packs** option selected or select the **Do not import management packs** option as appropriate. To import management packs manually after the installation, see section [“Manually importing included management packs”](#) on page 59.

When finished, click **Next**.

13. In the Install Product screen, click **Install** to begin installation.



- When the installation is complete, click **Finish** in the Finish Setup screen to exit the Wizard.



Verification

Do the following:

- Go to **Control Panel** and open the **Programs and Features** utility.
- Check if HYCU SCOM Management Pack for F5 BIG-IP is present in the list.
- Mandatory when Data Collector has been installed. Do the following:
 - Go to **Control Panel**, navigate to System and **Security > Administrative Tools**, and double-click **Services**.
 - Verify that the following entry is present in the Name column: HYCU SCOM Data Collector for F5 BIG-IP
 - Verify that the value in the Status column reads Running.
- Mandatory when management packs have been imported. In the SCOM Operations console, in the **Monitoring** view, check if the **F5 BIG-IP (by HYCU)** folder contains elements as shown in the following figure:

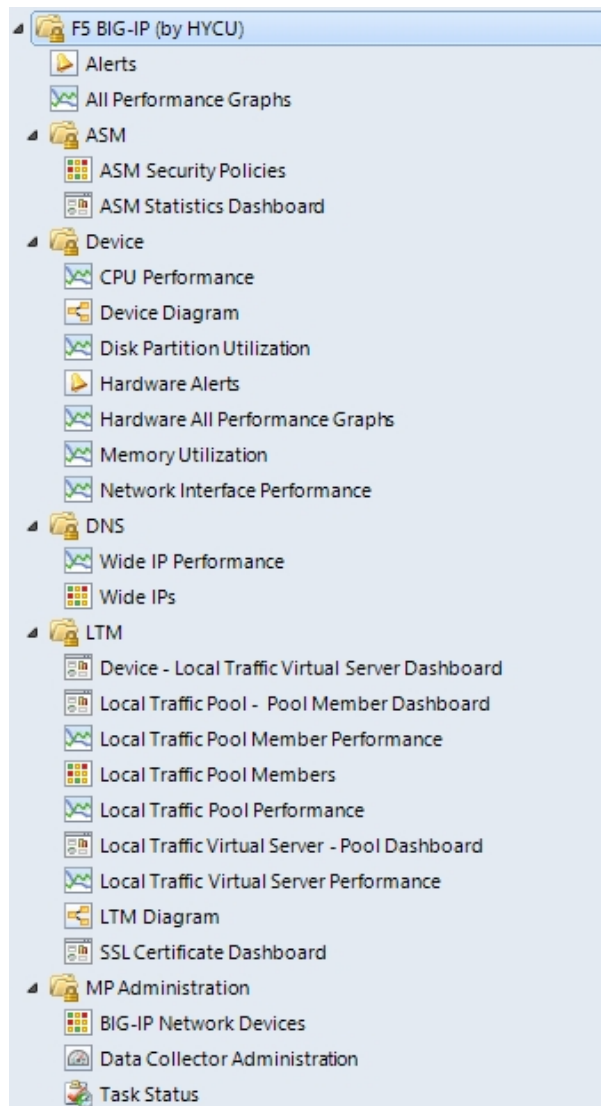


Figure 2-1: Elements of SCOM MP for F5 BIG-IP, as seen in the SCOM Operations console

If the depicted elements are present in your SCOM Operations console, the included management packs have been successfully imported into SCOM.

5. Mandatory when management packs have been imported. In the SCOM Operations console, in the **Reporting** view, check if the following reports are present in the respective folders:

HYCU Management Pack for F5 BIG-IP ASM (Reports):

- ASM Attacks
- ASM User Sessions

HYCU Management Pack for F5 BIG-IP Device (Reports):

- Device Performance
- Device Traffic Report

- Inbound License Utilization (Top N)
- Outbound License Utilization (Top N)

HYCU Management Pack for F5 BIG-IP LTM (Reports):


- Virtual Server Traffic Report

Configuring HYCU F5 BIG-IP Device Action Account with SCOM Operations console

HYCU F5 BIG-IP Device Action Account is required by the Data Collector to access BIG-IP devices through BIG-IP iControl REST API. You can configure the account by using:

- SCOM Operations console
To use this interface, complete the procedure documented in this section.
- Windows PowerShell
To use this interface, follow instructions in section [“Configuring HYCU F5 BIG-IP Device Action Account with Windows PowerShell” on page 61.](#)

To configure HYCU F5 BIG-IP Device Action Account from SCOM Operations console, do the following:

1. Log on to the SCOM management server where SCOM MP for F5 BIG-IP is installed, and start the SCOM Operations console.
2. In the **Administration** view, expand **Run As Configuration > Accounts**.
3. In the Task pane, under Actions, click **Create Run As Account**.
4. In the Create Run As Account Wizard, click **Next**.
5. In the General Properties page, select **Basic Authentication** for the Run As account type option. Enter a value for the **Display name** option, and then click **Next**.
 **Note** Selection for the Run As account does not depend on the user account type that is configured as the monitoring user account for a particular BIG-IP device.
6. In the Credentials page, type credentials of the user account that you created in section [“Configuring monitoring user accounts” on page 11](#), and then click **Next**.
7. In the Distribution Security page, select the **More secure - I want to manually select the computers to which the credentials will be distributed** option.
8. Click **Create** to create the user account and close the wizard.

To assign the user account to BIG-IP devices, do the following

1. Log on to the SCOM management server with administrative privileges and start the SCOM Operations console.
2. In the **Administration** view, click **Run As Configuration > Profiles**, and then double-click **HYCU F5 BIG-IP Device Action Account**.

3. In the Run As Account Wizard dialog box, select **Run As Accounts**, and then click **Add**.
4. In the Run As account drop-down list, choose the previously added account, and then select the **A selected class, group, or object** option.
5. Click **Select**, and then select **Object**.
6. In the Look for drop-down list, select **Node**, and then click **Search** to start the search for network devices.
7. Add BIG-IP devices discovered as network devices (select them in the Available items list, then click **Add**), and click **OK** to save configuration.

The Run As Profile Wizard window should resemble the figure that follows.

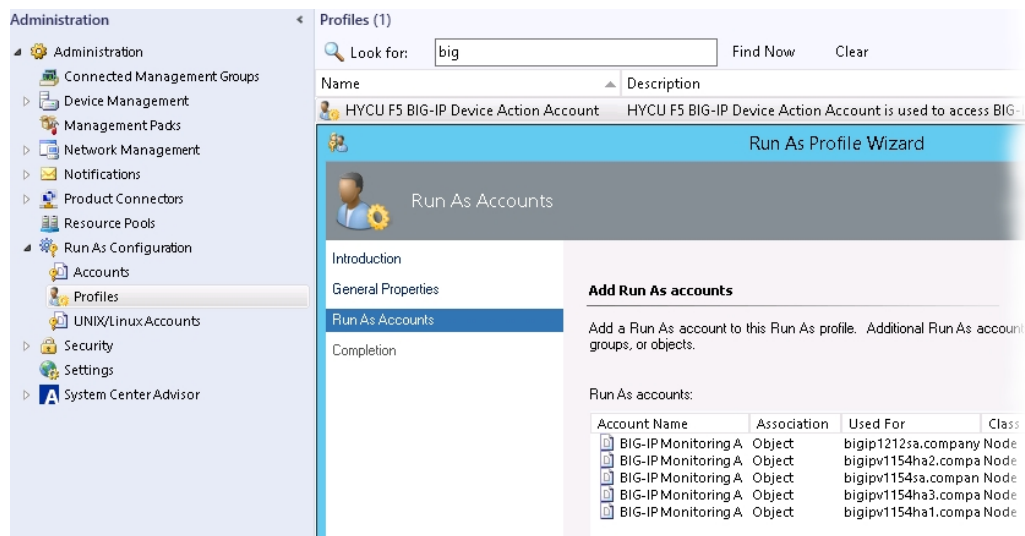


Figure 2-2: Assigning HYCU F5 BIG-IP Device Action Account for F5 BIG-IP devices discovered as network devices

8. Specify account distribution to one or more SCOM resource pools where the network devices are discovered.
9. Complete the account assignment process.

Verification

Do the following:

1. In the SCOM Operations console, in the **Monitoring** view, expand **F5 BIG-IP (by HYCU) > MP Administration**.
2. Select **BIG-IP Network Devices**.
3. Check if the network devices (discovered through iControl REST API) are present in the BIG-IQ Network Devices list.

This is a prerequisite for the license activation procedure.

Configuring HYCU F5 BIG-IP default port

To configure HYCU F5 BIG-IP default port from the SCOM Operations console, do the following:

1. Log on to the SCOM management server where SCOM MP for F5 BIG-IP is installed, and start the SCOM Operations console.
2. In the **Authoring** view, expand **Object Discoveries**.
3. In the **Object Discoveries**, find **F5 BIG-IP** and **F5 BIG-IP Extended Discovery**.
4. Right-click it and click on **Overrides**, select **Override the Object Discovery**. Then select **For all objects of class: Node** if you want to change the default port for all your discovered devices, or select **For a specific object of class: Node** if you want to change the default port for a specific device.
5. Override **Port** parameter with the new value.
6. Press on **“OK”** or **“Apply”** to apply the new port.

Setting up Data Warehouse Action Account for F5 BIG-IP devices

To allow access to DW Operations database for ASM Event Requests Data Rule, Data Warehouse Account profile needs to be set up.

Assign accounts for F5 Sync Failover Groups:

1. Log on the SCOM management server as a user with administrative privileges and start the SCOM Operations console.
2. In the **Administration** view, click **Run As Configuration > Profiles**, and then double-click **Data Warehouse Account**.
3. In the Run As Profile Wizard dialog box, select **Run As Accounts**, and then click **Add**.
4. In the Run As account drop-down list, select **Data Warehouse Action Account**, and then select the **A selected class, group, or object** option.
5. Click **Select**, and then select **Class**.
6. In the **Filter by** text box, enter F5 Sync Failover Group. Click **Search**. In the Available items list, select **F5 Sync Failover Group**, and then click **OK** to save configuration.

The Run As Profile Wizard window should resemble the figure that follows.

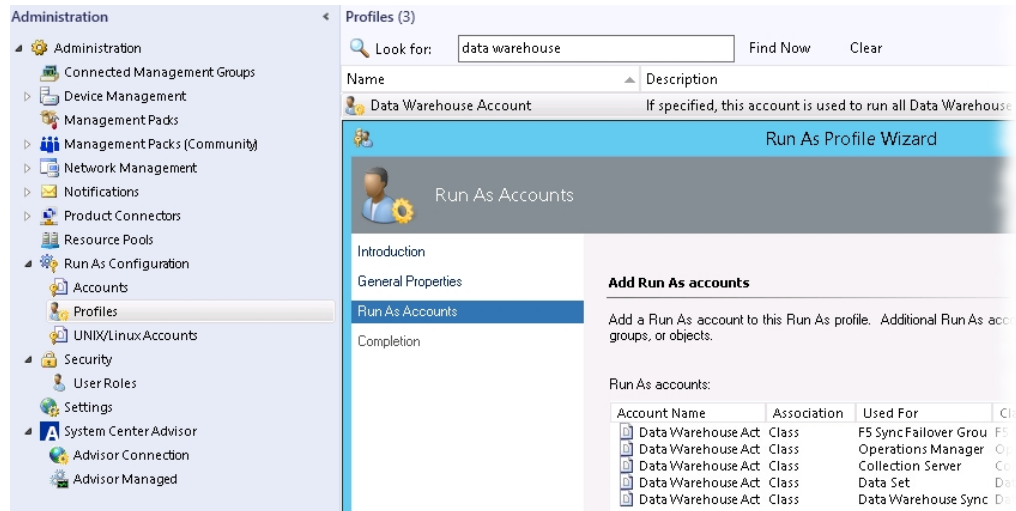


Figure 2-3: Assigning Data Warehouse Action Account

7. Complete the account assignment process.

Note Make sure that under **Run As Configuration > Accounts > Data Warehouse Action Account > Distribution > Selected computers**, "All Management Servers Resource Pool" is listed under the "Selected computers" table, in order to guarantee that all SCOM management servers have access to the Data Warehouse.

Compliance with Federal Information Processing Standards (FIPS)


HYCU SCOM Management Pack for F5 BIG-IP does not require special configuration steps for operation in environments that are compliant with the FIPS 140-2 standard. Such environments include the following:

- Microsoft Windows operating system where the security setting for FIPS compliance is enabled in the effective policy
- Microsoft System Center Operations Manager that is running in FIPS-compliant mode

Chapter 3

Upgrade

This chapter provides information on how to upgrade an earlier version of SCOM MP for F5 BIG-IP to this product version.

 **Important** A new format of license activation file was introduced in product version 4.3. If you are upgrading from an earlier version, you will require assistance from HYCU Customer Support to complete the process.

To upgrade the product, follow the steps:

1. Depending on the product version from which you are upgrading, do the following:

SCOM MP for F5 BIG-IP version 3.0 or later:

In-place upgrade is supported, and its procedure is the same as new installation procedure. During the in-place upgrade, entire configuration of SCOM MP for F5 BIG-IP in SCOM is preserved, and the included management packs are upgraded. To upgrade the product, follow instructions in chapter *Installation and configuration*, section [“Installing the product” on page 18](#).

SCOM MP for F5 BIG-IP version earlier than 3.0:

In-place upgrade is not supported. Management packs, configuration, and performance data of SCOM MP for F5 BIG-IP in SCOM are not preserved. Follow instructions in appendix *Advanced tasks*, section [“Upgrading the product from a version earlier than 3.0” on page 58](#).

2. *Mandatory when upgrading from a SCOM MP for F5 BIG-IP version earlier than 4.3.* Contact HYCU Customer Support for assistance.
3. Once the ***SCOM MP for F5 BIG-IP*** upgrade is complete, it is recommended to restart the Microsoft Monitoring Agent service on all systems with HYCU SCOM Data Collector for F5 BIG-IP.

Chapter 4

Product licensing


This chapter explains different types of product licenses and provides instructions on how to obtain the license keys and activate your licenses.

Prerequisites for licensing tasks

Before performing licensing tasks for SCOM MP for F5 BIG-IP, make sure that the following prerequisites are fulfilled:

- Network devices which you plan to activate licensing for are discovered in SCOM and visible in its Monitoring view in the F5 BIG-IP (by HYCU) > MP Administration > BIG-IP Network Devices context.
- The following product features are installed on each SCOM management server of the SCOM resource pool that is dedicated for monitoring BIG-IP devices:
 - Data Collector

To determine such SCOM management servers, open the SCOM Operations console, go to the Monitoring view, and navigate to the **F5 BIG-IP (by HYCU) > MP Administration > Data Collector Administration** context.

 **Note** The system where SCOM MP for F5 BIG-IP is installed does not require Internet connectivity when the product license is activated (the license key is applied).

Activating software evaluation and universal licenses

For software evaluation and universal licenses, the license activations files are provided to you by HYCU Customer Support.

To activate your license, do the following on each SCOM management server in the SCOM resource pool that is being used to monitor BIG-IP devices (and has HYCU SCOM Data Collector for F5 BIG-IP installed):

- Copy `mpbigip_licact_new.dat` file to the ProgramData path on the SCOM server (default location: `%ProgramData%\Comtrade\Comtrade F5 Data collector`).

Verification

Do the following:

1. Check if the `mpbigip_licact_new.dat` file exists in the ProgramData path (default location: `%ProgramData%\Comtrade\Comtrade F5 Data collector`).
2. Wait for five minutes.
3. Check if `mpbigip_licact_new.dat` has been renamed to `mpbigip_licact.dat`.
The renamed file indicates that the BIG-IP devices are visible to SCOM and HYCU SCOM Data Collector for F5 BIG-IP is receiving SCOM requests properly.

Activating perpetual (permanent) licenses

The perpetual (permanent) license activation procedure depends on the range of BIG-IP devices you want to include in the license request.

Generating license request files for all unlicensed devices

To generate license request file for all unlicensed BIG-IP devices, perform the following steps on any of the SCOM management servers monitoring BIG-IP devices and has HYCU SCOM Data Collector for F5 BIG-IP installed:

1. From Start menu/screen launch Windows PowerShell and navigate to the Program Files directory (default location: `C:\Program Files (x86)\Comtrade Software\HYCU SCOM MP for F5 BIG-IP\Licensing PowerShell scripts`).
The specified location of the Licensing PowerShell scripts directory is the default location.

Example

```
cd 'C:\Program Files (x86)\Comtrade Software\HYCU SCOM MP for F5 BIG-IP\Licensing PowerShell scripts'
```

2. To generate license request file (`mpbigip_license_requests.dat`), and save it to the desired location on disk, run the `CreateRequestFile.ps1` command, pass company name and path where request file should be saved.

Example

```
.\CreateRequestFile.ps1 'company name' 'C:\'
```

3. To activate the license request file, open a web browser and go to the [Licensing Portal | HYCU](#) webpage.

Register and upload previously saved license request file. The system should automatically process your request.

You should receive the license activation file `mpbigip_licact_new.dat` by e-mail within 10 minutes.

Save it to an appropriate location.

Generating license request files for individual devices

To generate license request file for desired BIG-IP devices, do the following on any of the SCOM management servers monitoring BIG-IP devices and has HYCU SCOM Data Collector for F5 BIG-IP installed:

1. From Start menu/screen launch Windows PowerShell and navigate to the Program Files directory (default location: C:\Program Files (x86)\Comtrade Software\HYCU SCOM MP for F5 BIG-IP\Licensing PowerShell scripts). The specified location of the Licensing PowerShell scripts directory is the default location.


Example

```
cd C:\Program Files (x86)\Comtrade Software\HYCU SCOM MP for F5 BIG-IP\Licensing PowerShell scripts
```

2. To generate license request file (mpbigip_license_requests.dat), and save it to the desired location on disk, run the CreateRequestFile.ps1 command, pass company name and path where request file should be saved and list of BIG-IP Management addresses of devices that should be licensed.

Example

```
\CreateRequestFileForSpecifiedBigIpDevices.ps1 'company name' 'C:\' '10.81.12.164', '10.81.12.165'
```

 **Note** User running the CreateRequestFileForSpecifiedBigIpDevices.ps1 script should have write permissions on a directory where the request file is to be created, or the command should be run with administrator privileges.

This command should be executed by providing parameters in the order as specified in the example.

Activation keys for perpetual (permanent) licenses are node-locked and they are activated during product installation and configuration steps.

Applying license activation files

To activate your license, do the following on each SCOM management server in the SCOM resource pool that is being used to monitor BIG-IP devices:


1. Copy the new license file mpbigip_liact_new.dat on this SCOM management server on appropriate location if it does not already exist.
2. After successful activation, when Data Collector detects new license file, it converts it to mpbigip_liact.dat or merges it with the previous one if it already exists.

Verification

Do the following:

1. Check if the `mpbigip_licact_new.dat` file exists in the ProgramData directory (default location: `%ProgramData%\Comtrade\Comtrade F5 Data collector`).
2. Wait for five minutes.
3. Check if `mpbigip_licact_new.dat` has been renamed to `mpbigip_licact.dat`.
The renamed file indicates that the BIG-IP devices are visible to SCOM and HYCU SCOM Data Collector for F5 BIG-IP is receiving SCOM requests properly.

Devices and its configuration objects can be discovered without a valid license, but monitors and rules provided by HYCU SCOM Management Pack for F5 BIG-IP cannot function in such circumstances.

 **Note** An improperly performed license activation procedure has an effect on the product's monitoring functionality in general. Monitors and rules provided by SCOM MP for F5 BIG-IP do not function without a valid license.

Chapter 5

Functionality overview

This chapter contains an overview and detailed description of each SCOM MP for F5 BIG-IP feature.

General product functionality

Alerts

Alerts view provides an overview of all active alerts related to the BIG-IP devices and applications delivered using BIG-IP devices. Some of the scenarios when HYCU SCOM Management Pack for F5 BIG-IP creates alerts are the following:

- Device does not have enough free storage space
- CPU utilization is high
- Local traffic virtual servers, local traffic pools, or local traffic pool members are marked unavailable, or their status is unknown.

All Performance Graphs

This folder contains performance data graphs, such as CPU Performance, Disk Partition Utilization, Memory Utilization, Network Interface Performance, Local Traffic Virtual Server Performance, Local Traffic Pool Performance, Local Traffic, and Pool Member Performance.

MP Administration

BIG-IP Network Devices shows all devices discovered by HYCU SCOM Management Pack for F5 BIG-IP.

Data Collector Administration pane enables Data Collector service management. HYCU SCOM Data Collector for F5 BIG-IP and HYCU SCOM Data Collector for F5 BIG-IP Service Tasks are listed in Task Pane.

HYCU Management Pack for F5 BIG-IP Device (Core)

This management pack locates issues in the BIG-IP device hardware components:

- CPU cores
- Disk partitions
- TMM memory
- Other memory
- Network interfaces

Device performance views

This folder contains performance data graphs, such as CPU Performance, Disk Partition Utilization, Memory Utilization, Network Interface Performance, and All Hardware Performance.

Device Diagram

Device Diagram view displays topology view of the discovered BIG-IP devices along with its related Hardware objects, some of which are: CPU cores, disk partitions, TMM memory, other memory, and network interfaces.

Hardware Alerts

Hardware Alerts view provides an overview of all active alerts related to the hardware components (CPU Cores, Disk partitions, Memory, and Network Interfaces) of BIG-IP devices.

HYCU Management Pack for F5 BIG-IP Device (Reports)

To access BIG-IP device reports, do the following:

1. In the **Monitoring** pane, expand **Monitoring** and click **F5 BIG-IP (by HYCU)**.
2. Select a BIG-IP device in one of the following views:
 - **MP Administration > BIG-IP Network Devices**
 - **Device > Device Diagram View**
 - **LTM > LTM Diagram View**
 - **LTM > Device - Local Traffic Virtual Server Dashboard**

3. In **Task pane**, choose one of the available BIG-IP Device Reports:

- **Device Performance**


This report displays the effect of user activity on the F5 BIG-IP device throughput and consumption of the device resources: CPU, memory, and disk. You can narrow the scope of data analysis to customizable business hours.

- **Device Traffic Report**

This report shows traffic details on a specific BIG-IP device. You can choose to show traffic only during business hours, and select the time and days of the week of your business cycle.


- **Inbound License Utilization (Top N)**

This report shows license inbound utilization details for a specific device. You can choose algorithms from the drop-down list (Top N or Bottom N).


 **Note** The report contains no data unless the Inbound License Utilization (in %) (Performance DB DW) rule is enabled.

- **Outbound License Utilization (Top N)**

This report shows license outbound utilization details for a specific device. You can choose algorithms from the drop-down list (Top N or Bottom N).

 **Note** The report contains no data unless the Outbound License Utilization (in %) (Performance DB DW) rule is enabled.

By selecting Top N algorithm, from either of the two reports, you can identify which devices utilize their license the most and you can plan ahead if you are going to need a better license by identifying growth trends on the report. By selecting Bottom N you can identify which devices utilize their license the least, and you can organize where your applications are deployed to better utilize this license

 **Note** License utilization reports are only available for F5 BIG-IP versions 12.1.x and later.

HYCU Management Pack for F5 BIG-IP LTM (Core)

This management pack locates issues in the LTM infrastructure (virtual servers, pools, pool members), applications which are affected and discovers unutilized resources.

Dashboards

- Device - Local Traffic Virtual Server Dashboard presents relationships between devices and virtual servers that the device contains.
- Local Traffic Pool - Pool Member Dashboard presents relationships between pools and pool members.
- Local Traffic Pool Members shows all Pool Members.
- Local Traffic Virtual Server - Pool Dashboard presents relationships between virtual servers and pools.
- SSL Certificate state view presents SSL certificate instances.

LTM performance views

This folder contains performance data graphs, such as Local Traffic Virtual Server Performance, Local Traffic Pool Performance, Local Traffic, and Pool Member Performance.

LTM Diagram

LTM Diagram view displays topology view of the discovered BIG-IP devices along with its related LTM and Hardware objects, some of which are: traffic groups, devices (active and passive), local traffic virtual servers, local traffic pools, and local traffic pool members.

Filtering virtual servers, pools, and pool members

It is possible to exclude or monitor only specific virtual servers, pools, and pool members with the **F5 Sync Failover Group Discovery**. Use parameter **Ignore Pattern** to exclude discovery and monitoring of objects that match specified pattern. Use parameter **Include Pattern** to discover only those objects that match specified pattern. If both filters are used, Ignore Pattern takes precedence over Include Pattern. The virtual server, pool, and pool member names refer to the values as displayed on the BIG-IP device.

1. In the **Authoring** pane, expand **Authoring > Management Pack Objects > Object Discoveries**.
2. In the Object Discoveries list, search for and right-click **F5 Sync Failover Group Discovery**.
3. In the shortcut menu, select **Overrides > Override the Object Discovery > For all objects of class: HYCU F5 BIG-IP Applications**.
4. Depending on whether it is easier to limit monitoring with exclusion or inclusion override:
 - a. Ignore parameter

In the **Override Properties** dialog box, select the **Override** option next to the **Ignore Pattern** parameter.

In the **Override Value** column, enter regular expression matching names of objects that should not be monitored.

 **Note** Pattern matching is case sensitive.

Example

```
^test_|Test12
```

This pattern excludes all virtual servers, pools, and pool members beginning with "test_" OR containing "Test12" in their names. Matched objects are not discovered and therefore not monitored.

Example

```
^Test12$|^Test99$
```

This pattern excludes all virtual servers, pools, and pool members whose names are identical to either "Test12" or "Test99".

b. Include parameter

In the **Override Properties** dialog box, select the **Override** option next to the **Include Pattern** parameter.

In the **Override Value** column, enter regular expression matching names of objects that should be monitored.

 **Note** Pattern matching is case sensitive.

Example

```
^test_|Test12
```

With this pattern only virtual servers, pools, and pool members beginning with "test_" OR contain "Test12" in their names are discovered and monitored.

5. Click **OK**.

HA monitoring

SCOM MP for F5 BIG-IP discovers traffic groups on the BIG-IP device that contain at least one virtual server. These traffic groups are visible in LTM Diagram View. Virtual servers that are contained within that traffic group is shown in the diagram. Furthermore, it is possible to easily identify which devices are active and which are passive for that specific traffic group that is being displayed.

SCOM MP for F5 BIG-IP also monitors the health of a Sync Failover group. There are three monitors for Sync Failover Group:

- Number of available devices in Sync Failover Group is below threshold - This monitor checks if number of available devices in Sync Failover group is lower than predefined threshold. Monitor considers all devices that are in active or standby state available, and devices that are in any other state unavailable.
- Inconsistent states are reported for devices in Sync Failover Group - This monitor checks if devices that are in the targeted sync failover group report the same state for each other.
- F5 Sync Failover Group Configuration Monitor - This monitor checks if configuration within F5 BIG-IP devices in Sync Failover Group is synchronized. Configuration not being in sync might cause unexpected behavior such as applications not being available to end users.
- Sync Failover Group is not available for monitoring - This monitor checks if a Sync Failover group is available for monitoring. There are several reasons why a Sync Failover group could be unavailable for monitoring some of which are:

- All BIG-IP devices from targeted Sync Failover group are offline and their status cannot be obtained.
- All BIG-IP devices from targeted Sync Failover group cannot be reached, because of connectivity issues between the SCOM management server and the BIG-IP device.
- All BIG-IP devices from targeted cannot be reached because HYCU SCOM Data Collector for F5 BIG-IP has been stopped.
- SCOM MP for F5 BIG-IP license was not applied for all BIG-IP devices from targeted Sync Failover group.

HYCU Management Pack for F5 BIG-IP LTM (Reports)

To access BIG-IP LTM reports, do the following:

1. In the **Monitoring** pane, expand **Monitoring** and click **F5 BIG-IP (by HYCU) > LTM**.
2. Select a Virtual Server in one of the following views:
 - LTM Diagram View
 - Device - Local Traffic Virtual Server Dashboard
 - Local Traffic Virtual Server – Pool Dashboard
3. In **Task pane > Report Tasks** choose **Virtual Server Traffic Report**

This report shows traffic details on a specific Virtual Server. You can choose to show traffic only during business hours, and select time and days of the week of your business cycle.

HYCU Management Pack for F5 BIG-IP ASM (Core)

This management pack identifies if application attack is in progress and visualizes attacks history.

ASM Statistics Dashboard

BIG-IP Application Security Manager (ASM) protects against OWASP top 10 threats, application vulnerabilities, and zero-day attacks. Choose a device from device list which have ASM module, and then choose all virtual servers configured on that device or a specific virtual server identified by its full name.


Charts contain following statistical information:

- Number of blocked sessions
- Number of alarmed sessions

- Number of transactions
- Number of Brute Force attacks
- Number of Web Scraping attacks

ASM Security Policies

ASM Security Policies view shows all ASM policies.

-  **Note** The following properties are not available in F5 BIG-IP versions earlier than 11.6.0:
- Login Enforcement
 - Brute Force Attack Prevention Reference
 - Geolocation Enforcement
 - Session Tracking Statuses
 - Login Pages
 - IP Intelligence
 - CSRF Settings

HYCU Management Pack for F5 BIG-IP ASM (Reports)

In Reporting pane, click HYCU Management Pack for F5 BIG-IP ASM Reports. Available reports are as follows:

- ASM Attacks

This report summarizes ASM attack attempts that occurred in the selected period of time. It presents charts with five most frequent attack types, requested URLs, and request origins (countries, IP addresses). The report also includes tables with a complete list of attack attempts, grouped by attack type, together with corresponding details.
- ASM User Sessions

This report shows details about all user sessions marked as illegal by ASM on a selected F5 BIG-IP device, filtered by a specific support ID, attack type, and request origin (country and IP address).

HYCU Management Pack for F5 BIG-IP DNS (Core)

Some of the F5 BIG-IP Devices in F5 DNS Sync Group are not in sync monitor

Monitors if all BIG-IP Devices in F5 DNS Sync Group are in sync.

DNS Wide IP Performance view

This view contains DNS Wide IP performance data graphs.

Wide IPs view

Wide IPs view shows all Wide IPs and their health states

Filtering DNS objects

1. In **Authoring** pane, navigate to **Management Pack Objects > Object Discoveries**.
2. Right-click **F5 DNS Sync Group** Discovery, and select **Overrides > Override the Object Discovery > For all objects of class: All F5 DNS Wide IPs group**
3. Override Ignore Pattern parameter with a regular expression.

Example

test_

This pattern excludes all Wide IPs which name contains "test_". Ignore Pattern parameter is case sensitive. Identified objects are neither discovered nor monitored.

4. Find Include Pattern parameter and check its Override checkbox. Fill Override Value cell with a regular expression.

If name of DNS configuration object matches Include Pattern, but does not match Ignore Pattern, it is discovered in SCOM. If the name of DNS configuration object matches both Include and Ignore Pattern is not discovered in SCOM.

Chapter 6

BIG-IP objects, properties, and relationships

SCOM MP for F5 BIG-IP discovers BIG-IP objects, their statuses, and relationships between them and renders them visible in the SCOM Operations console.

Depending on the actual configuration of your BIG-IP infrastructure, objects listed in the following tables are discovered and displayed at the specified locations within the **F5 BIG-IP (by HYCU)** context of the **Monitoring** view.

BIG-IP devices

Device > Device Diagram

LTM > Device – Local Traffic Virtual Server Dashboard

LTM > LTM Diagram

MP Administration > BIG-IP Network Devices

BIG-IP CPU cores, disk partitions, memory units, and network interfaces

Device > Device Diagram

LTM > LTM Diagram

F5 LTM traffic groups

LTM > LTM Diagram

F5 LTM traffic group devices, active groups, and passive groups

LTM > LTM Diagram

F5 LTM virtual servers

LTM > Device – Local Traffic Virtual Server Dashboard

LTM > Local Traffic Virtual Server – Pool Dashboard

LTM > LTM Diagram

F5 LTM pools (and their relationships with LTM virtual servers)

LTM > Local Traffic Virtual Server – Pool Dashboard

LTM > LTM Diagram

F5 LTM pool members (and their relationships with LTM pools)

LTM > LTM Diagram

LTM > Local Traffic Pool Members

LTM > Local Traffic Pool – Pool Members Dashboard

LTM > Local Traffic Virtual Server – Pool Dashboard

HYCU SCOM Data Collector for F5 BIG-IP services (and the related alerts)

MP Administration > Data Collector Administration

BIG-IP SSL certificates

LTM > SSL Certificate Dashboard

LTM > LTM Diagram

BIG-IP ASM security policies

ASM > ASM Security Policies

ASM > ASM Statistics Dashboard

BIG-IP DNS wide IPs

ASM > ASM Security Policies

BIG-IP device- and device component-related alerts

Alerts

Recent SCOM MP for F5 BIG-IP tasks (statuses)

MP Administration > Task Status

Chapter 7

Uninstallation

This chapter contains instructions on how to completely uninstall HYCU SCOM Management Pack for F5 BIG-IP (SCOM MP for F5 BIG-IP) from your environment.

Uninstallation overview

To uninstall SCOM MP for F5 BIG-IP, complete the following tasks on each SCOM management server where the product is installed:

1. Remove management packs included in SCOM MP for F5 BIG-IP.
2. Uninstall SCOM MP for F5 BIG-IP.

Removing included management packs

To remove management packs included in SCOM MP for F5 BIG-IP and other product references from the SCOM management server, do the following:


1. Launch the SCOM Operations console and connect to the management server.
2. In the **Administration** view, click **Management Packs**.
3. Remove reference to `HYCU.SC.COM.MP.F5.BIG-IP` from the `Microsoft.SystemCenter.SecureReferenceOverride` management pack:
 - a. Export the management pack.
 - b. Make a copy of the file you exported the management pack to.
 - c. Edit the file copy and remove all dependencies on the SCOM MP for F5 BIG-IP configuration from it. Search for `Comtrade.F5.BigIp` and delete the containing references, then save your changes.
 - d. Delete the management pack from SCOM.
 - e. Import back the management pack from the edited file copy.
4. In the Management Packs pane, right-click the management pack you want to remove, and then click **Delete**. Remove the included management packs in the following order:
 - a. HYCU Management Pack for F5 BIG-IP ASM (Reports)
 - b. HYCU Management Pack for F5 BIG-IP ASM (Core)
 - c. HYCU Management Pack for F5 BIG-IP DNS (Core)
 - d. HYCU Management Pack for F5 BIG-IP LTM (Reports)

- e. HYCU Management Pack for F5 BIG-IP LTM (Core)
- f. HYCU Management Pack for F5 BIG-IP Device (Reports)
- g. HYCU Management Pack for F5 BIG-IP Device (Core)

Uninstalling SCOM MP for F5 BIG-IP from management server


To uninstall SCOM MP for F5 BIG-IP, do the following:

1. In Windows Control Panel, select **Programs > Programs and Features**.
2. Locate and right-click the **HYCU SCOM Management Pack for F5 BIG-IP** entry, then select **Uninstall**.

 **Note** A warning dialog box may appear informing you that other users are logged in to this computer. You cannot completely remove this program if another user is currently running it.

3. In the Setup Wizard, follow instructions until the uninstallation process completes.

Setup Wizard cannot remove the files that were placed to the installation directories after the installation, for example, license files or configuration files. You can delete such files after Setup Wizard completes the uninstallation process.

 **Note** To manually delete any files from the installation directories after the SCOM MP for F5 BIG-IP uninstallation, first make sure that these files are not used by other programs and their deletion does not cause issues.

Chapter 8

Troubleshooting

If you encounter problems with using SCOM MP for F5 BIG-IP, you can often solve them yourself. This chapter contains information that may help you in such cases.

General troubleshooting guidelines

When investigating an issue, first verify that:

- All installation prerequisites are fulfilled and the product is configured according to the provided instructions.
- You are not running into a known product limitation. For a list of the limitations, see the *HYCU SCOM Management Pack for F5 BIG-IP Release Notes*.
- Your issue is not related to third-party software or hardware (F5 or Microsoft). Otherwise, contact the respective vendor for assistance.
- You have the latest operating system and software application patches installed on the affected systems. Else, install the patches and check if the issue persists.
- The affected systems are not running out of memory or storage space.

Problems and solutions

This section lists symptoms of common problems that you may encounter while using SCOM MP for F5 BIG-IP, together with proposed actions – resolution steps.

Registry key access failure during product upgrade

Symptoms

Event with ID 16010 and a message similar to the following is logged into the operating system event log:

```
MPBigIpGenericPropertyBagExtendedProbe.js : Issue with taking property
InstallDir from registry. Error message:Invalid root in registry key
"HKLM\SOFTWARE\Wow6432Node\Comtrade\BIG-IP MP\InstallDir
```

Possible resolution steps

While SCOM MP for F5 BIG-IP is being upgraded, product-specific keys and values are deleted from Windows registry and later created again. SCOM workflows may fail to access

those entities in the upgrade timeframe.

Do the following:

1. Wait for the upgrade to complete. If the problem persists, proceed to the next step.
2. Check if registry keys from the event log messages actually exist; their absence denotes an incomplete product installation. If the registry keys are missing, proceed to the next step.
3. Reinstall SCOM MP for F5 BIG-IP.

REST query to a BIG-IP device results in an error

Symptoms

When verifying configuration of a monitoring user account that has administrative privileges, after you access the following webpage and supply the user account credentials, iControl REST API prompts for the credentials again or responds with the 401

Authentication Required message:

```
https://<IPaddress>/mgmt/tm/cm/device?$select=version,managementIp
```

In this instance, <IPaddress> is the management IP address of the BIG-IP device.

Possible resolution steps

The problem might have one of the following causes:

- Supplied credentials are invalid.
- Monitoring user account has not been properly configured.

Check the following (and take appropriate corrective actions):

- Existence of a monitoring user account on the BIG-IP device
- Credentials that you supplied while configuring the monitoring user account
- Whether the monitoring user account has the Administrator role assigned

BIG-IP devices are not discovered

Case 1

Symptoms

One or more BIG-IP devices are not discovered and are missing in the corresponding context of the SCOM Operations console (the Monitoring > F5 BIG-IP (by HYCU) > MP Administration > BIG-IP Network Devices view).

Possible resolution steps

Do the following for each missing BIG-IP device:

1. Check if the device is discovered by SCOM as a network device. In the SCOM, go to the **Administration** view and expand **Network Management > Network Devices**.
 If the device is not already discovered as a network device, follow instructions in section [“Workflows are not triggered”](#) on page 50.
 If the device is already discovered as a network device, proceed to the next step.
2. Check its System Object ID property in the Network Device Properties window.

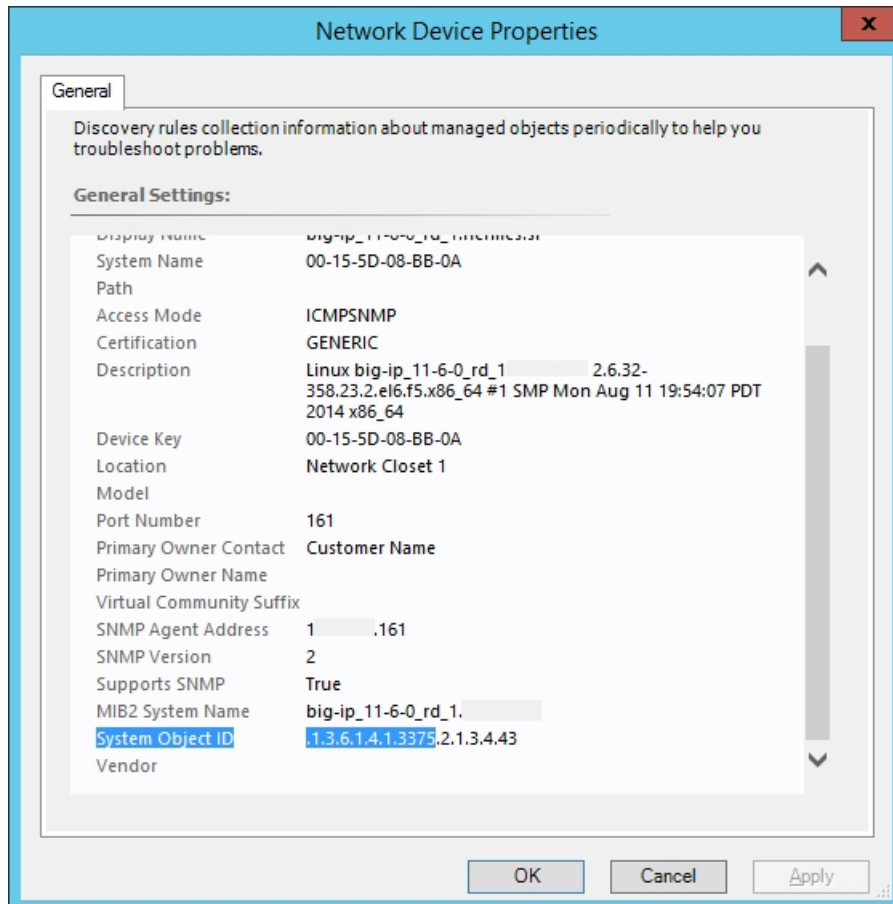


Figure 8-1: SCOM Operations console showing BIG-IP device properties

If the System Object ID value does not start with the .1.3.6.1.4.1.3375 prefix, proceed as follows:

- a. Log in to the BIG-IP Configuration Utility (web user interface).
- b. In the left pane, expand **System > Software Management > Hotfix List** and select **Import**. Locate, import, and install the latest hotfix for your BIG-IP product version.
- c. Set the boot location to the appropriate disk volume.
- d. In the left pane, expand **System > Configuration > Device > General** and click **Reboot** to restart the device.
- e. Rediscover the device as a network device in SCOM.

- f. Override the BIG-IP device discovery to force SCOM MP for F5 BIG-IP to rediscover the device.

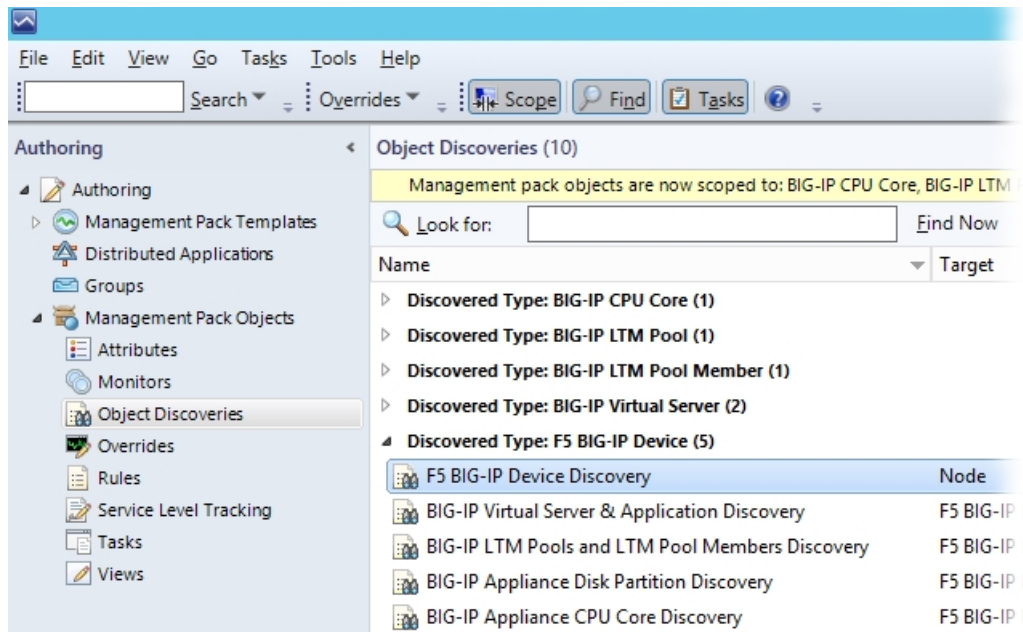


Figure 8-2: Discovered F5 BIG-IP devices listed in the SCOM Operations console

If the System Object ID value starts with the .1.3.6.1.4.1.3375 prefix, proceed to the next step.

3. Check if SCOM MP for F5 BIG-IP is installed on all required SCOM management servers. See section [“Installation and configuration” on page 18](#).

If the installation is correct, proceed to the next step.

4. Check if HYCU F5 BIG-IP Device Action Account is configured correctly in SCOM. See section [“Configuring HYCU F5 BIG-IP Device Action Account with SCOM Operations console” on page 25](#).

If the configuration is correct, proceed to the next step.

5. Check if a local BIG-IP user account with administrative privileges is used for HYCU F5 BIG-IP Device Action Account.

If the chosen user account is proper, proceed to the next step.

6. Check if the device accepts iControl REST API calls from the Data Collector (HYCU SCOM Data Collector for F5 BIG-IP service) and that the device can communicate with the SCOM MP for F5 BIG-IP host system by using the HTTPS protocol through port 443.

Example

Check if the following URL is accessible from the Data Collector host system:

```
https://<BIGIPdeviceAddress>/mgmt/tm/cm/device
```

Case 2

Symptoms

BIG-IP devices are not discovered. They are visible in neither of the following SCOM Operations console contexts of the Monitoring view:

- F5 BIG-IP (by HYCU) > Device > Device Diagram
- F5 BIG-IP (by HYCU) > MP Administration > BIG-IP Network Devices

Possible resolution steps

Do the following:

1. Verify that the BIG-IP devices are configured for monitoring. See section [“Configuring SNMP access to BIG-IP devices” on page 9](#). If the devices are properly configured, proceed to the next step,
2. Check if HYCU BIG-IP Device Action Account is configured. See section [“Configuring HYCU F5 BIG-IP Device Action Account with SCOM Operations console” on page 25](#).

Workflows are not triggered

Case 1

Symptoms

No discovery, monitor, or rule workflow for SCOM MP for F5 BIG-IP is triggered on a SCOM management server.

Possible resolution steps

There may be pending updates for Windows Server or System Center Operations Manager on the SCOM management server. In this case, install the updates and restart the system.

Case 2

Symptoms

SCOM MP for F5 BIG-IP monitors or rules appear to be functioning only for certain objects. For example, some of the discovered virtual servers are being monitored while others are not and their health status indicators are not set.

Possible resolution steps

BIG-IP iControl REST API service that monitors BIG-IP devices might not respond to the SCOM MP for F5 BIG-IP requests correctly or in time for the particular objects.

If the BIG-IP device is a standalone device, restart the iControl REST API service. Do the following:

1. Log in to the BIG-IP device through the command-line interface.
2. In the BIG-IP Traffic Management Shell (tmsh), run the following command:

```
restart /sys service icrd
```

Alerts are not generated or performance data is not collected

Symptoms

BIG-IP objects are not being monitored, their performance data is not collected, and their health status indicators keep being set to Healthy.

Possible resolution steps

Check if the product license is activated. For instructions on how to activate it, see chapter [“Product licensing” on page 30](#).

To list all licensed BIG-IP devices, do the following:

1. Open a Windows PowerShell window.
2. Run the following command:

```
set-location "${Env:ProgramFiles(x86)}\Comtrade Software\HYCU SCOM MP  
for F5 BIG-IP\Licensing PowerShell scripts"
```

3. Run the following command:

```
.\LicensedBigIPDevices.ps1
```

ASM Statistics Dashboard is not available in the SCOM web console

Symptoms

ASM Statistics Dashboard is not available in the SCOM web console.

Possible resolution steps

None. ASM Statistics dashboard is not compatible with the SCOM web console.

ASM Statistics Dashboard is empty

Symptoms

You notice the following:

- ASM Statistics Dashboard does not display any data.
- Events with IDs 31569, 31557, 31552, 31563, and 31561 keep being logged into the operating system event log.
- Event with ID 31551 and a message similar to the following keeps being logged into the operating system event log:

```

Failed to store data in the Data Warehouse. The operation will be
retried.
Exception 'SqlException': Cannot open database "OperationsManagerDW"
requested by the login. The login failed.
Login failed for user '<DomainName>\<UserName>'.
One or more workflows were affected by this.
Workflow name: Comtrade.F5.BigIp.ASM.Event.RequestsRule
Instance name: <InstanceFQDN>
Instance ID: {<UUID>}
Management group: <GroupName>

```

Possible resolution steps

Check if Data Warehouse Action Account is configured properly. For instructions on how to set it up, see section ["Setting up Data Warehouse Action Account for F5 BIG-IP devices" on page 27.](#)

Some virtual servers are missing in ASM Statistics Dashboard

Symptoms

Data for specific virtual servers is missing in ASM Statistics Dashboard.

Possible resolution steps

HYCU Management Pack for F5 BIG-IP ASM (Core) collects statistics about attacks that are detected by the ASM module by using iControl REST API. For illegal request data to be accessible through iControl REST API, a log profile must be configured on the local traffic virtual server.

Do the following:

1. Log in to the BIG-IP Configuration Utility (web user interface).
2. In the left pane, expand **Local Traffic** and click **Virtual Servers**. In the virtual server list, select the affected virtual server.
3. In the upper toolbar, select **Security > Policies**.
4. Set the Log Profile option to **Enabled**.
5. Move the **Log illegal requests** entry from the Available list to the Selected list.
6. Click **Update**.

Self IP Address property is empty

Symptoms

The Self IP Address device property is not set on an F5 BIG-IP device.

Possible resolution steps

To populate the property, restart the BIG-IP iControl REST API service. Run the following commands:

```
tmssh stop sys service restjavad
tmssh start sys service restjavad
```

Rest Framework Version and Is Virtual properties are empty

Symptoms

The Rest Framework Version and Is Virtual device properties are not set on an F5 BIG-IP device.

Possible resolution steps

None. iControl Rest API of the listed BIG-IP version does not support these properties.

Health recalculation does not change the monitor's health indicator

Symptoms

The Recalculate Health dialog box of the SCOM Health Explorer reports a completed health recalculation, but the recalculation process does not have any effect on the monitor's health status indicator.

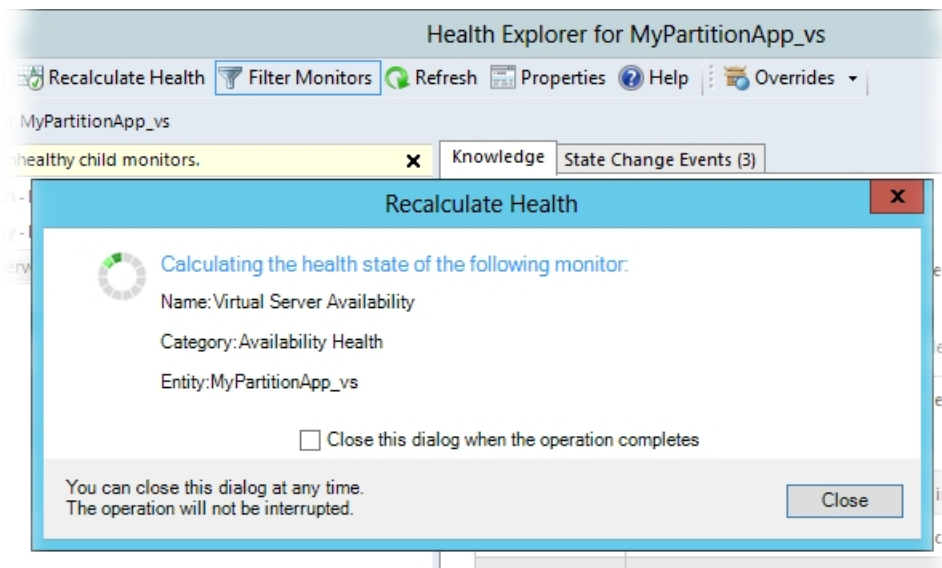


Figure 8-3: Health Explorer with progress indicator of health recalculation

Possible resolution steps

Use the Reset Health option to set the monitor's health status indicator back to Healthy.

Getting assistance


Depending on the required type of assistance, do the following:

- If you need assistance with product evaluation, contact your HYCU account owner or sales representative.
- If you have already purchased the product, you have a valid support agreement, and:
 - You need assistance with *product licensing*, see section “[Licensing assistance](#)” below.
 - You have *an issue with the product or your monitored environment*, see section “[Support](#)” below.

Licensing assistance

Depending on the service that you need, do the following:

- To generate license request files and activate licenses, follow instructions in chapter “[Product licensing](#)” on page 30.
- To change license scope and arrange any license management activities, contact your HYCU sales representative at the info@hycu.com email address.
- To redesignate licenses (deactivate existing licenses), go to the [Licensing Portal | HYCU](#) website. Sign in to your account and follow the License Redesignation steps.
- For any licensing-related issues or questions about the licensing process, send an email with detailed issue description (expected behavior, symptoms, screen shots, log files, and similar) or list of questions to info@hycu.com.

 **Note** Make sure to include your company name and purchase order (PO) number in communication with HYCU Customer Support.

Support

If you have an issue with the product or your monitored environment, collect the following data before contacting the Customer Support department:


- General information:
 - Your company name
 - Purchase order (PO) number
- Basic information about the environment such as:
 - Host operating system
 - System Center Operations Manager version
 - F5 BIG-IP version
 - Version of the installed SCOM MP for F5 BIG-IP (the product)
 - Whether you are still evaluating the product or already using a purchased license
 - Whether the product is installed in a development or production environment

- Additional information such as:
 - Whether the product was installed or it was upgraded from an earlier version
 - Time when the product was installed
 - Time when the product was most recently reconfigured
 - Time when you first noticed issue symptoms
 - Versions of the monitored applications
 - Operating systems on which monitored applications are running
 - Whether the host operating system or monitored environment were updated recently
- Detailed explanation of the issue, including:
 - Expected behavior
 - Issue symptoms
 - Screen shots of the user interfaces
 - List of troubleshooting actions that you have already taken

The listed pieces of information are required by HYCU Customer Support so that a support engineer can efficiently investigate the issue from the very beginning. Pack the data collection into an archive, and do one of the following:

- *Preferred.* On the [HYCU](#) webpage, submit your request (support case) with the archive attached.
- Send an email with the attached archive to support@hycu.com.

HYCU Customer Support will contact you shortly.

 **Important** If the email attachment is too large or the email is getting rejected by the company email server, deliver the archive using your preferred file sharing facility and contact HYCU support to share the details.

Getting additional information and latest updates

For additional information about SCOM MP for F5 BIG-IP, its latest product version, and up-to-date documentation, go to the [F5 Monitoring - HYCU](#) webpage.


Before contacting HYCU Customer Support

If you cannot solve your issue, report it. Before contacting HYCU Customer Support, make sure that:

- You perform the general checks. For details, see section [“Troubleshooting” on page 46](#).
- You verify that your problem is not documented in this chapter. For more information, see section [“Problems and solutions” on page 46](#).
- You collect relevant data that might be required to send to HYCU Customer Support: a

description of your problem, configuration specification of your environment, and similar information. For details, see section [“Customer Support” on page 69](#).

The HYCU Customer Support team will provide you with further instructions. Among other things, you may be asked to perform diagnostic operations in your environment and collect specific data from your systems and send it to HYCU.

 **Note** The HYCU Customer Support team is not qualified to solve the issues related to third-party software or hardware.

For information on how to reach HYCU Customer Support, see part [“HYCU Customer Support and information” on page 69](#).

Appendix A


Advanced tasks

Installing the product in quiet mode or passive mode

With quiet installation or passive installation, the following typical features are installed by using default installation parameters:

- Data Collector
- Device management pack
- Device Reports management pack
- DNS management pack
- LTM management pack
- ASM management pack
- ASM Reports management pack
- Support tool
- Licensing module

Default port value for HYCU SCOM Data Collector for F5 BIG-IP is 19703. This port is used during quiet installations and passive installations. When running a quiet or passive installation, management packs are imported, which means that quiet installations and passive installations should be performed only on SCOM management servers.

 **Note** Quiet and passive modes of installation can be also used for upgrading the product except for upgrades from SCOM MP for F5 BIG-IP versions earlier than 3.0.

Quiet installation

Quiet installation installs SCOM MP for F5 BIG-IP without displaying the progress status and without requiring user input.

To install the product in quiet mode, do the following:

1. On the SCOM management server, open a Command Prompt window with administrative privileges.
2. Change the current directory to the directory where the `HYCU.SCOM.MP.F5.BIG-IP.msi` file is located.

Example

A command line that changes the current directory:

```
cd D:\temp
```

3. Run the following command:

```
msiexec.exe /i HYCU.SCOM.MP.F5.BIG-IP.msi /quiet
```

Continue the process with product configuration by following instructions in section [“Configuring HYCU F5 BIG-IP Device Action Account with SCOM Operations console” on page 25.](#)

Passive installation

Passive installation installs SCOM MP for F5 BIG-IP in unattended mode. In this mode, installation progress status is displayed, but you are not prompted for option selections or confirmations.

To install the product in passive mode, do the following:

1. On the SCOM management server, open a Command Prompt window with administrative privileges.
2. Change the current directory to the directory where the HYCU.SCOM.MP.F5.BIG-IP.msi file is located.

Example

A command line that changes the current directory:

```
cd D:\temp
```

3. Run the following command:

```
msiexec.exe /i HYCU.SCOM.MP.F5.BIG-IP.msi /passive
```

Continue the process with product configuration by following instructions in section [“Configuring HYCU F5 BIG-IP Device Action Account with SCOM Operations console” on page 25.](#)

Upgrading the product from a version earlier than 3.0

To upgrade the product from a version earlier than 3.0, do the following:

1. Uninstall the earlier version of SCOM MP for F5 BIG-IP. For instructions, see the *User Guide* of that product version.

2. To install the new product version, follow instructions in section [“Installing the product” on page 18.](#)
3. Continue the process by configuring the product as instructed in section [“Configuring HYCU F5 BIG-IP Device Action Account with SCOM Operations console” on page 25.](#)

Manually importing included management packs

To import the management packs included in the product into SCOM, do the following:

1. Log on to the SCOM management server¹ and start the SCOM Operations console.
2. In the **Administration** view, click **Management Packs**.
3. In the Actions task pane, select **Import management packs**.
4. Locate the management pack and click **Open**.

Default management packs location:

```
%ProgramFiles(x86)%\Comtrade Software\HYCU SCOM MP for F5 BIG-IP\Management packs
```

5. Import

```
HYCU.SC.COM.MP.F5.BIG-IP.ASM.mpb
HYCU.SC.COM.MP.F5.BIG-IP.Device.Reports.mpb
HYCU.SC.COM.MP.F5.BIG-IP.DNS.mpb
HYCU.SC.COM.MP.F5.BIG-IP.LTM.mpb
HYCU.SC.COM.MP.F5.BIG-IP.LTM.Reports.mpb
HYCU.SC.COM.MP.F5.BIG-IP.mpb
HYCU.SC.COM.MP.F5.BIG-IP.Reports.mpb
```

6. Click **Install** to complete the import procedure.

If the same version of any management pack has already been imported, the SCOM Operations console reports the following information:

```
“A management pack contained in HYCU SCOM Management Pack for F5 BIG-IP bundle (version <Major>.<Minor>.<BuildNumber>) has already been imported”
```

Continue the installation and configuration process by following instructions in section [“Configuring HYCU F5 BIG-IP Device Action Account with SCOM Operations console” on page 25.](#)

¹ SCOM management server where any Management pack feature of SCOM MP for F5 BIG-IP is installed.

Creating a management pack for overrides

Most vendor management packs are sealed for changes so it is not possible to change any of the original settings in the management pack file. However, customizations can be created, such as overrides or new monitoring objects, and saved to a different management pack. By default, System Center Operations Manager saves all customizations to the default management pack. As a best practice, create a separate management pack for each sealed management pack you want to customize.

Creating a new management pack for storing overrides has the following advantages:

- It simplifies the process of customizations export created in your test and pre-production environments to your production environment. For example, instead of exporting the default management pack containing customizations from multiple management packs, you can export the management pack containing customizations of a single management pack.
- You can delete the original management pack without first needing to delete the default management pack. A management pack containing customizations is dependent on the original management pack. This dependency requires deleting the management pack with customizations before deleting the original management pack. If all of your customizations are saved to the default management pack, export the default management pack, delete the customizations from the default management pack and reimport the default management pack again before deleting the management pack.
- It is easier to track and to update customizations of individual management packs.

Putting BIG-IP devices into maintenance mode

When you need to put F5 BIG-IP devices offline for their maintenance, you must also properly change the mode of the corresponding discovered devices in SCOM. Maintenance mode in SCOM enables you to suspend monitoring operations in order to avoid false alerts and errors while the devices are undergoing maintenance.

To put a F5 BIG-IP device into the maintenance mode in SCOM, do the following:


1. In the SCOM Operations console, in the **Monitoring** view, expand **F5 BIG-IP (by HYCU)**.
2. Expand **Device** and then click **Device Diagram**.
3. In the Device Diagram pane, right-click the F5 BIG-IP device, go to **Maintenance Mode**, and then select **Start Maintenance Mode**.
4. In the Maintenance Mode Settings dialog box, ensure that the **Selected objects and all their contained objects** option is selected and then click **OK**.

To put an entire Sync-Failover Group, including all associated F5 BIG-IP devices, into the maintenance mode in SCOM, do the following:

1. In the SCOM Operations console, in the **Monitoring** view, expand **Discovered Inventory**.
2. In the Tasks pane, under State Actions, click **Change Target Type**.
3. In the Select Items to Target dialog box, click **View all targets** and then select **F5 SyncFailover Group** from the target list. Click **OK**.
4. In the Discovered Inventory pane, right-click the Sync Failover Group, go to **Maintenance Mode**, and then select **Start Maintenance Mode**.
5. In the Maintenance Mode Settings dialog box, ensure that the **Selected objects and all their contained objects** option is selected and then click **OK**.

Configuring HYCU F5 BIG-IP Device Action Account with Windows PowerShell

Configuring HYCU F5 BIG-IP Device Action Account by using Windows PowerShell includes running the `bigIpRunAsAccountAndProfileSetup.ps1` script that is bundled with SCOM MP for F5 BIG-IP.

 **Important** `bigIpRunAsAccountAndProfileSetup.ps1` uses All Management Servers Resource Pool to distribute user accounts. This SCOM resource pool does not include SCOM gateway servers. If your SCOM deployment includes gateway servers, choose a custom SCOM resource pool for user account distribution.

This script automatically configures Data Warehouse Action Account in SCOM. For more information, see section [“Setting up Data Warehouse Action Account for F5 BIG-IP devices” on page 27](#).

To prepare command-line environment for Run As account setup and distribution (procedures in the next sections), do the following:

1. On the SCOM management server, launch Windows PowerShell.
2. Change the current directory to the `Configuration Tools` subdirectory within the installation directory of the included management packs.

Example

```
cd 'C:\Program Files (x86)\Comtrade Software\HYCU SCOM MP for F5 BIG-IP\Management packs\Configuration Tools'
```


Distributing Run As accounts to all SCOM management servers

To set up Run As accounts and distribute them to all SCOM management servers, do the following:

1. Create a plain text file containing the fully qualified domain name (FQDN), user name, and password for each BIG-IP device in the following format:

```
<FQDN1>, <UserName1>, <Password1>
<FQDN2>, <UserName2>, <Password2>
<FQDN3>, <UserName3>, <Password3>
```

Make sure there is no empty line at the end of the file.

 **Tip** Instead of creating a new file, modify the `exampleFQDNandCredentialsFile.txt` file that is located in the same directory.

2. In Windows PowerShell, run one of the following commands:
 - To allow the script to ask for a confirmation before performing changes, run the following command:

```
bigIpRunAsAccountAndProfileSetup.ps1 -FQDNandCredentialsFile
<FQDNandCredentialsFile>
```

- To force the script to perform changes without asking for a confirmation, run the following command:

```
bigIpRunAsAccountAndProfileSetup.ps1 -FQDNandCredentialsFile
<FQDNandCredentialsFile> -DistributeToAll
```

In these instances, `<FQDNandCredentialsFile>` is the full path of the file that you created in step 1.


Distributing Run As accounts to a specific SCOM resource pool

To set up Run As accounts and distribute them to all SCOM management servers of a specific SCOM resource pool, do the following:

1. Create a plain text file containing the fully qualified domain name (FQDN), user name, and password for each BIG-IP device in the following format:

```
<FQDN1>, <UserName1>, <Password1>
<FQDN2>, <UserName2>, <Password2>
<FQDN3>, <UserName3>, <Password3>
```

Make sure there is no empty line at the end of the file.

 **Tip** Instead of creating a new file, modify the `exampleFQDNAndCredentialsFile.txt` file that is located in the same directory.

2. In Windows PowerShell, run the following command:

```
bigIpRunAsAccountAndProfileSetup.ps1 -FQDNAndCredentialsFile
<FQDNandCredentialsFile> -ResourcePoolName <ResourcePool>
```

In this instance, `<FQDNandCredentialsFile>` is the full path of the file that you created in step 1, and `<ResourcePool>` is the name of the SCOM resource pool whose SCOM management servers you want to distribute Run As account to.


Verifying Run As accounts

To verify that the Run As account credentials for each device are correct, do the following:

1. Create a plain text file containing the fully qualified domain name (FQDN), user name, and password for each BIG-IP device in the following format:

```
<FQDN1>,<UserName1>,<Password1>
<FQDN2>,<UserName2>,<Password2>
<FQDN3>,<UserName3>,<Password3>
```


Make sure there is no empty line at the end of the file.

 **Tip** Instead of creating a new file, modify the `exampleFQDNAndCredentialsFile.txt` file that is located in the same directory.

2. In Windows PowerShell, run the following command:

```
bigIpRunAsAccountAndProfileSetup.ps1 -FQDNAndCredentialsFile
<FQDNandCredentialsFile> -TestCredentials
```

In this instance, `<FQDNandCredentialsFile>` is the full path of the file that you created in step 1.

 **Note** HYCU F5 BIG-IP Device Action Account is not associated with BIG-IP devices for which the corresponding credentials are incorrect.

Advanced script usage

In relation to using the `bigIpRunAsAccountAndProfileSetup.ps1` script, this section instructs you how to:

- Use a parameter value separator other than comma
- Run the script outside the SCOM management server

Using parameter value separators other than comma

If the user names or passwords contain comma (,), you can use a different separator character.

Do the following:

1. Create a plain text file containing the fully qualified domain name (FQDN), user name, and password for each BIG-IP device in the following format:


```
<FQDN1><Separator><UserName1><SeparatorChar><Password1>
<FQDN2><Separator><UserName2><SeparatorChar><Password1>
<FQDN3><Separator><UserName3><SeparatorChar><Password1>
```

In this instance, *<Separator>* is a character other than comma that separates parameter values.

Make sure there is no empty line at the end of the file.

Example

```
<FQDN1>;<UserName1>;<Password1>
<FQDN2>;<UserName2>;<Password2>
<FQDN3>;<UserName3>;<Password3>
```

 **Tip** Instead of creating a new file, modify the `exampleFQDNandCredentialsFile.txt` file that is located in the same directory.

2. In Windows PowerShell, run the following command:

```
bigIpRunAsAccountAndProfileSetup.ps1 -FQDNandCredentialsFile
<FQDNandCredentialsFile> -Separator "<Separator>"
```

In this instance, *<FQDNandCredentialsFile>* is the full path of the file that you created in step 1, and *<Separator>* is the separator character that you used in the file.

Example

```
bigIpRunAsAccountAndProfileSetup.ps1 -FQDNandCredentialsFile
C:\myCredentialsFile.txt -Separator ";"
```

Running the script outside the SCOM management server

If you are unable to run the `bigIpRunAsAccountAndProfileSetup.ps1` script on a desired SCOM management server, you can do so on an arbitrary system where SCOM MP for F5 BIG-IP is installed.

Do the following:

1. On the system where SCOM MP for F5 BIG-IP is installed, launch Windows PowerShell.
2. Change the current directory to the `Configuration Tools` subdirectory within the installation directory of the included management packs.


Example

```
cd 'C:\Program Files (x86)\Comtrade Software\HYCU SCOM MP for F5 BIG-IP\Management packs\Configuration Tools'
```

3. Create a file containing fully qualified domain name (FQDN), user name, and password for all BIG-IP devices in the following format:

```
<FQDN1>, <UserName1>, <Password1>
<FQDN2>, <UserName2>, <Password2>
<FQDN3>, <UserName3>, <Password3>
```

Make sure there is no empty line at the end of the file.

 **Tip** Instead of creating a new file, modify the `exampleFQDNandCredentialsFile.txt` file that is located in the same directory.

4. In Windows PowerShell, run one of the following:

- A command (prompts for user input):

```
bigIpRunAsAccountAndProfileSetup.ps1 -FQDNandCredentialsFile
<FQDNandCredentialsFile> -ManagementServerName <ManagementServer>
-ManagementServerCredentials (Get-Credential)
```

In the above instance, `<FQDNandCredentialsFile>` is the full path of the file that you created in step 3, and `<ManagementServer>` is the name of the SCOM management server that should execute script actions.

- A sequence of commands (do not prompt for user input):

```
$password = ConvertTo-SecureString -String <Password> -AsPlainText
-Force
$credentials = New-Object -TypeName
System.Management.Automation.PSCredential -ArgumentList
<DomainName>\<UserName>, $password
bigIpRunAsAccountAndProfileSetup.ps1 -FQDNandCredentialsFile
<FQDNandCredentialsFile> -ManagementServerName <ManagementServer>
-ManagementServerCredentials $credentials
```

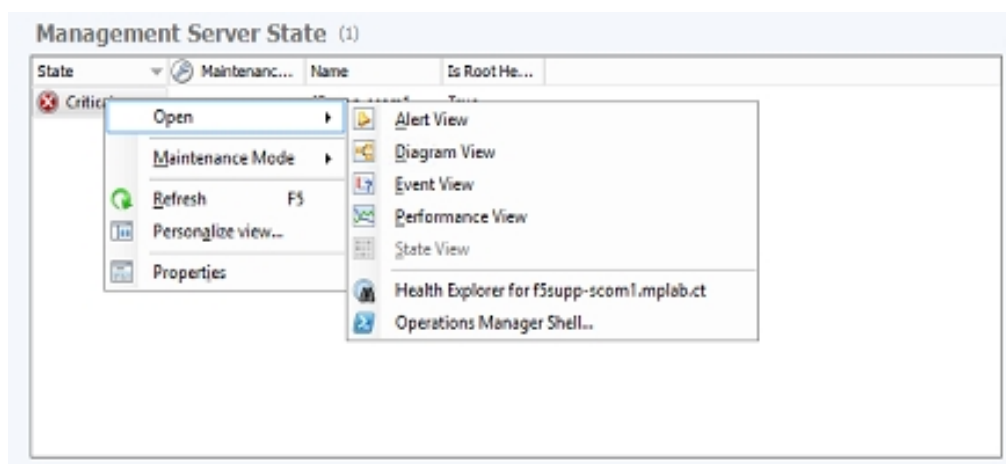
In the above instance, `<Password>`, `<DomainName>`, and `<UserName>` are credentials of the user account, `<FQDNandCredentialsFile>` is the full path of the file that you created in step 3, and `<ManagementServer>` is the name of the SCOM management server that should execute script actions.

Adjusting SCOM configuration for large environments

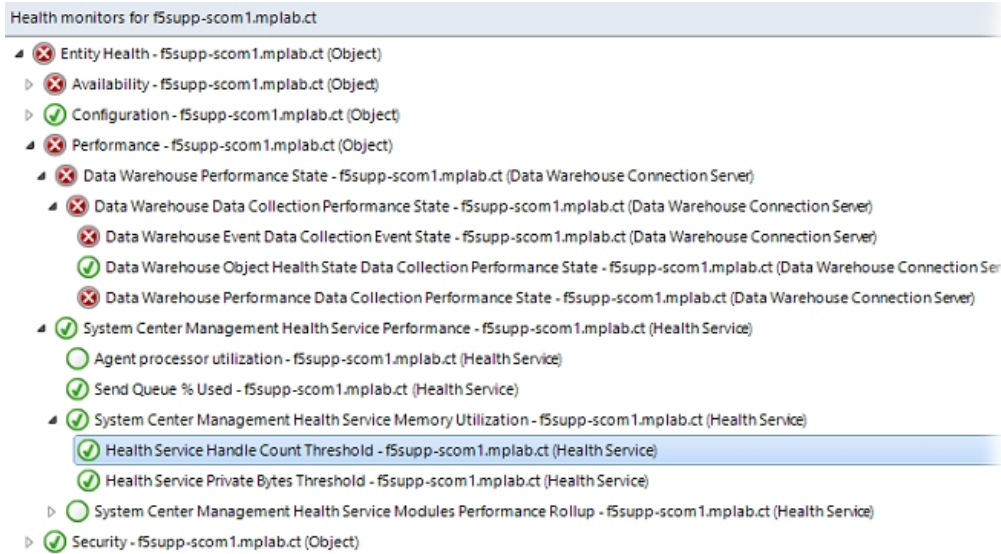
When monitoring large environments with System Center Operations Manager (SCOM), it is possible that SCOM services consume more resources than they usually do in an average-size environment. This may cause the services to restart which in turn stops monitoring for a certain period.

To prevent this from happening, certain overrides must be created in SCOM. Do the following:

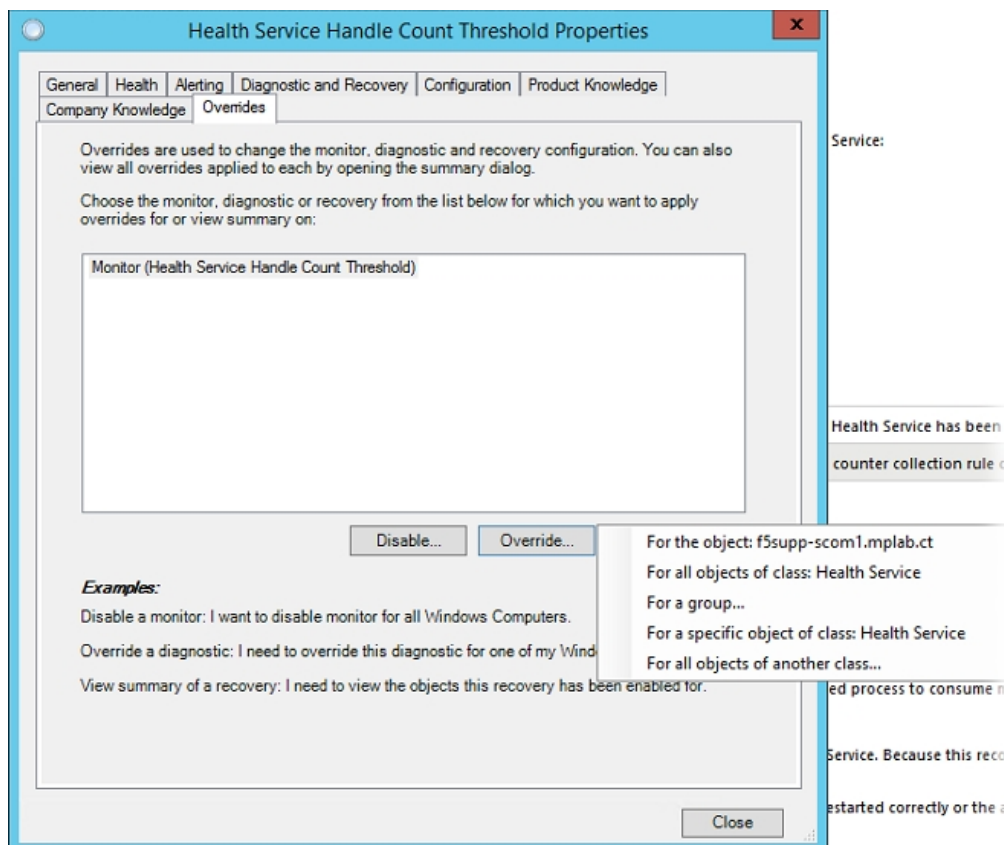
1. Open the SCOM Operations console.
2. Navigate to **Monitoring > Operations Manager > Management Server > Management Servers State**.
3. Right-click one of the SCOM management servers and open health explorer for it.



4. Clear the **Scope is only unhealthy child monitors** option to show all monitors.
5. Navigate to **Performance > System Center Management Health Service Performance > System Center Management Health Service Memory Utilization**.




6. Right-click **Health Service Handle Count Threshold** and select the **Monitor Properties** option.
7. Select the **Overrides** tab, click **Override**, and then select the **For all objects of class: Health Service** option.



8. Override the Agent Performance Monitor Type (Consecutive Samples) – Threshold parameter to 30,000.

9. Select a management pack that you wish to save this to and click **OK**.
10. Open the overrides for Health Service Private Bytes Threshold.
11. Override the Agent Performance Monitor Type (Consecutive Samples) – Threshold parameter to 6,442,450,944.
12. Select a management pack that you wish to save this to and click **OK**.

 **Note** Suggested thresholds (Agent Performance Monitor Type (Consecutive Samples) – Threshold and Agent Performance Monitor Type (Consecutive Samples) – Threshold) are calculated for a monitored environment with 150 BIG-IP devices.

Management packs used for these calculations are as follows:

- HYCU Management Pack for F5 BIG-IP Device (Core)
- HYCU Management Pack for F5 BIG-IP LTM (Core)
- HYCU Management Pack for F5 BIG-IP ASM (Core)
- HYCU Management Pack for F5 BIG-IP ASM (Reports)

HYCU Customer Support and information

Use the communication channels listed in this section if you need:

- Help with the product licensing process
- Assistance while using the product
- Additional information about this product
- Information about other HYCU products

Customer Support

Should you require additional information or assistance while using the product, contact the vendor that shipped it.

If you have purchased the product directly from HYCU, and are experiencing a problem, search for a solution on the following webpage:

support.hycu.com

In the absence of an article addressing your problem, ask HYCU Customer Support for assistance: on the webpage, click **Submit a request** and fill in the request form. You must be signed in with a valid account prior to submission. Apply for an account at the following email address:

support@hycu.com

Important: Before submitting a request to the Customer Support department, perform a health check on all systems that are in failed (critical, red) state and have the following information ready:

- Symptoms
- Sequence of events leading to the problem
- Commands and options that you used
- Messages you have received (a description with the date and time)

For a complete list of pieces of required support information, check troubleshooting sections in the product documentation.

Company website and video channel

For more information about our company and other products we offer, visit HYCU website at:

www.hycu.com

For additional information, watch videos on the HYCU channel on YouTube:

www.youtube.com/c/HYCUInc

General information

For questions related to product business or purchase of this or other HYCU products, send an email to:

info@hycu.com

Feedback

For comments or suggestions about this product, including its documentation, send an email to:

info@hycu.com

We will be glad to hear from you!

