



Installing patch IPD-57659



Ref.:	Installing patch IPD-57659
Version:	1.01
Product:	cyberelements Gate & Cleanroom
Date:	2026-09-10

Purpose:

This document describes the installation of security patch IPD-57659 for cyberelements Gate and Cleanroom on the applicable servers.

TABLE OF CONTENTS

1	Introduction	4
1.1	Target audience	4
1.2	Compatibility.....	4
2	Rolling out the security patch.....	5
3	Applying the security patch	6
4	Using API v1	7
5	Verifying that the security patch has been applied	8

1 Introduction

This document details the procedure for applying security patch IPD-57659 to the supported **cyberelements** Gate and Cleanroom Client Hosted servers.

The SaaS environments (cyberelements.io, Workroom Session Service and Cleanroom Session Service) have already been patched.

1.1 Target audience

Target audience		Comments
General public		
Partners/integrators		SSH access and root privileges on all Mediation Controllers are required.
End users		
Administrators		SSH access and root privileges on all Mediation Controllers are required.

1.2 Compatibility

The security patch applies to:

- All Mediation Controller servers (Standalone or Cluster architecture) from version 8.1 of **cyberelements** Gate (formerly Systancia Gate or IPdiva Secure).
- All Mediation Controller servers (Standalone or Cluster architecture) from version 4.4 of **cyberelements** Cleanroom (formerly Systancia Cleanroom).

2 Rolling out the security patch

Before applying the security patch to the supported servers, carry out the following action:

1. Back up or snapshot the machines on which the security patch will be applied.

Deployment of the fix is transparent to users and causes no service interruption. Allow approximately 5 minutes per machine to install the security fix: this is the installation time, not a production outage.

The security patch can be applied in parallel across all the machines concerned; no reboot of these machines is required once the security patch has been applied.

Before starting to apply the security patch, make sure you have the following:

- An SFTP file transfer tool (on Windows, WinSCP or FileZilla can be used).
- An SSH client (on Windows, PuTTY can be used).
- The connection details for each server, with both a standard user account and root.
- The SH script used to deploy the security patch.

3 Applying the security patch

On each applicable server, upload the file `2026_08_12_IPD-57659_Fix_Security.sh` to the `/tmp/` directory using an SFTP file transfer tool.

Special case — use of the integrity server: if such a server has been deployed, switch it to permissive mode before applying the security patch. To do so, connect to the integrity server over SSH and run the following command as root:

```
1 # /usr/local/ipdiva/iis/bin/ipdivaiisctrl.py enablepermissive
```

Connect over SSH to the servers on which the security patch is to be applied and switch to root. Start applying the security patch with the following command:

```
1 # bash /tmp/2026_08_12_IPD-57659_Fix_Security.sh
```

If the security patch was applied successfully, the following message is displayed:

```
SUCCESS: IPD-57659 applied (0 allowed IP(s) across all orgs)
```

If applying the security patch failed, collect the information displayed during the operation and send it to Systancia Support, then restore the backup or snapshot taken before the security patch was applied.

Special case — use of the integrity server: because components have been modified on the Mediation Controller side, the component hashes must be recalculated, after which permissive mode can be disabled. To do so, connect to the integrity server over SSH and run the following commands as root:

```
1 # /usr/local/ipdiva/iis/bin/ipdivaiisctrl.py updatehashes
2 # /usr/local/ipdiva/iis/bin/ipdivaiisctrl.py disablepermissive
```

At this point, the security patch has been applied.

4 Using API v1

If you use API v1, in particular for Gate for Workplace and Cleanroom Desk, the number of **allowed IP(s)** shown in the **SUCCESS** message when the security patch is applied may vary. This number corresponds to the number of IP addresses listed in the Allowed IP addresses field (« Adresses IP autorisées » in a French-language console) of the Gate API v1 domain.

In addition, **any change to the IP addresses entered in the API v1 domain requires the security fix to be reapplied**. You will therefore need to follow this entire procedure again after each change.

To check whether API v1 is in use, log in to the Gate administration console using the URL matching your version:

- Gate 8.9: https://<ADDR_MEDIATION>/gate/admin
- Gate 8.8 and earlier: https://<ADDR_MEDIATION>/mediation/local

Once logged in, go to the **Authentication > Domains** tab (« Authentification > Domaines » in a French-language console) and check whether the API v1 domain is present. If it is not present, API v1 is not in use.

When using Cleanroom Desk, if the message “No organization is configured, contact your administrator” (« Aucune organisation n’est paramétrée, contactez votre administrateur » in a French-language console) is displayed when accessing the Gate administration console, this also means that API v1 is not in use.

5 Verifying that the security patch has been applied

Once the security patch has been deployed on all Mediation Controller servers, you can check that the platform is no longer vulnerable using the following command:

```
1 # M=mediation.example.com; c=$(curl -sk -o /dev/null -w '%{http_code}' \
-H 'Content-Type: text/xml' --data-binary \
'<methodCall><methodName>api.getVersion</methodName></methodCall>' \
"https://$M/mediation/administration/authentication/action"); case $c in \
403) echo SAFE;; 2??) echo VULNERABLE;; *) echo "UNKNOWN ($c)";; esac
```

Replace `mediation.example.com` with the DNS name or the Web IP address of your Mediation Controller server.

In a Cluster architecture, run the command three times: once with the Web RIP of each of the two Mediation Controllers, then once with the Web VIP of the Cluster.

This command can be run from any Linux machine with access to the Web server of **cyberelements** Gate/Cleanroom.

If the server is correctly patched, the command returns `SAFE`. Conversely, if the server is vulnerable, it returns `VULNERABLE`.

If the command returns `UNKNOWN`, this may indicate that the DNS name cannot be resolved.

© **Systancia 2026** – All rights reserved

The information provided in this document is supplied for information purposes only and therefore does not constitute any commitment on the part of Systancia. This information may be changed by Systancia without notice.

This document is intended for experienced users with a basic knowledge of the Microsoft Windows Server operating system. Systancia cannot be held liable for handling errors made in the course of using this documentation. Any use made of this document is entirely at your own risk.

Third-party trademarks: all other trademarks, product names and company names mentioned in this document are cited for explanatory purposes and are the property of their respective owners. In particular, Microsoft and Windows Server are trademarks of Microsoft Corporation in the United States and other countries.

SYSTANCIA

Phone: 03 89 33 58 20

Fax: 03 89 33 58 21

Website: <https://www.sep.systancia.com>