

# Suggested Actions on WebSAMS

# Suggested Actions

---

- ❖ **Keep Latest Windows Security Update**
- ❖ **Check Windows Hardening Status**
- ❖ **Check Antivirus Protection Status**
- ❖ **Ensure System Backup In Order**
- ❖ **Keep Best Practice in System Operation**
- ❖ **Keep Latest HTTP Server Patch Update**

## Keep Latest Windows Update

---

Go to “Control Panel” > “Windows Update” then select:

- ❖ **Check for Updates**

(Select all updates except “Service Pack” / “Major Version Upgrade”)

- ❖ **View Update History**

- ❖ **Change Settings**

(“Check for updates but let me choose whether to download and install them”)

## Check Windows Hardening Status

- Refer to

*“Installation Guidelines for WebSAMS 3.0”*

➤ *“Appendix 7 : Windows Server 2012 R2 – OS Hardening Guide”*

<http://www.websams.edb.gov.hk/files/newschool/Doc%2033%20Installation%20Guidelines%20for%20WebSAMS%203.0%20V1.3.3.pdf>

**for Checking the Windows Hardening Status  
including:**

- ❖ Local Security Policy
- ❖ Windows Firewall
- ❖ Screen Saver Timeout  
*(On resume, display logon screen)*
- ❖ Remote Desktop with Network Level Authentication  
*(In normal operation, the remote desktop should be disabled)*

## Check Antivirus Protection Status

---

- ☑ Ensure the Antivirus Software is in latest version
- ☑ Ensure the Online Protection is enabled
- ☑ Ensure the Virus Pattern is up-to-date

## Ensure System Backup In Order

- Ensure the following kinds of backup are included:
  - Windows Server (Regular System Backup)
  - WebSAMS Program and Data (Daily, Weekly and Monthly Backup)
- Ensure encryption of backup image
- Check the Backup Log timely
- Check the status of Backup Media timely including:
  - On-line media (NAS)
  - Off-line media

## Keep Best Practice on System Operation

---

- **DO NOT share the disk storage of WebSAMS Server as network drive**
- **Only install WebSAMS related software**
- **DO NOT enable remote desktop service or install similar software**
- **DO NOT visit any suspected / unknown website or download files from questionable source in WebSAMS Server**

## Keep Latest HTTP Server Patch Update

- Run the following command every month:

*starthsp*



## ● Security Guides & Checklist for WebSAMS:

<http://cdr.websams.edb.gov.hk> > 主頁 > 參考資料 > 保安及處理敏感數據指引



網上校管系統資料庫  
WebSAMS Central Document Repository

主頁      最新消息      重要資訊      課程訊息

主頁 > 參考資料 > 保安及處理敏感數據指引

- 如何使用WebSAMS新增的系統保安設定檢查功能  
[下載 / Download](#)
- [Tackling Ransomware and Related Seminar \(17-05-2017\)](#)  
2017年5月15日香港電腦保安事故協調中心-保安公告的聯遞系統訊息  
CDS message on Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) - Security Bulletin (15-05-2017)  
[下載 / Download](#)
- 安裝網上校管系統的系統保安簡介  
[下載 / Download](#)
- 「網上校管系統」系統保安簡介及基本安全措施  
WebSAMS Security Guide and Recommended Practice  
[下載 / Download](#)
- System Security Setting Checklist for WebSAMS  
[下載 / Download](#)
- 「網上校管系統」伺服器、網絡管理及系統保安」重點分享 2017  
Seminar on Highlights of WebSAMS Server, Network & Security 2017  
詳情下載: [PPT格式](#) [PDF格式](#)
- 棄置/更換「網上校管系統」伺服器-處理敏感性數據指引  
[下載 / Download](#)

## ● Security Check for WebSAMS:

系統保安 > 保安檢查



The screenshot shows the 'Security Check' configuration page in the WebSAMS system. The left sidebar contains a navigation menu with 'System Security' expanded and 'Security Check' selected. The main content area is titled '[S-SEC23-01] 系統保安 > 保安檢查'. It includes a 'Daily Security Check' section with radio buttons for 'Start' (selected) and 'Stop'. Below this is a 'Options' section with a 'Check Time' dropdown set to '20:00 (hh:mm)' and a note that checks should not be scheduled during system backup periods. A checkbox for 'Send notification when abnormal reports are generated during the check' is checked. The 'NAS IP Address' field is highlighted with a red box and contains the value 'websams'. Below it, the 'Firewall Rule Name' field also contains 'websams'. At the bottom, there are buttons for 'Reset', 'Save', 'Save and Execute Scan', and 'Report Storage'. A summary section shows the results of a check performed on 30/08/2017 at 18:05, reporting 4 items on the WebSAMS server, 0 on the HTTP server, and 0 on the WebSAMS router. A note at the bottom provides additional documentation references.

[S-SEC23-01] 系統保安 > 保安檢查

每天保安檢查

啟動  停止

選項

檢查時間 20 : 00 (hh:mm)

系統檢查不應安排在每天系統備份期內進行

當檢查中產生異常報告時發出通知。

在「網上校管系統」伺服器中Windows Server 2012設定的補充資料

連接 NAS 的 IP 位址

防火牆規則名稱

websams

有關"防火牆規則名稱"細節，請參考"Doc 33 - Installation Guidelines for WebSAMS 3.0" - Appendix 7 Section D。

重設 儲存 儲存及執行掃描 報告存庫

保安檢查摘要 (於 30/08/2017 18:05)

在異常報告中，

在WebSAMS伺服器找到4個項目；

在HTTP伺服器找到0個項目；

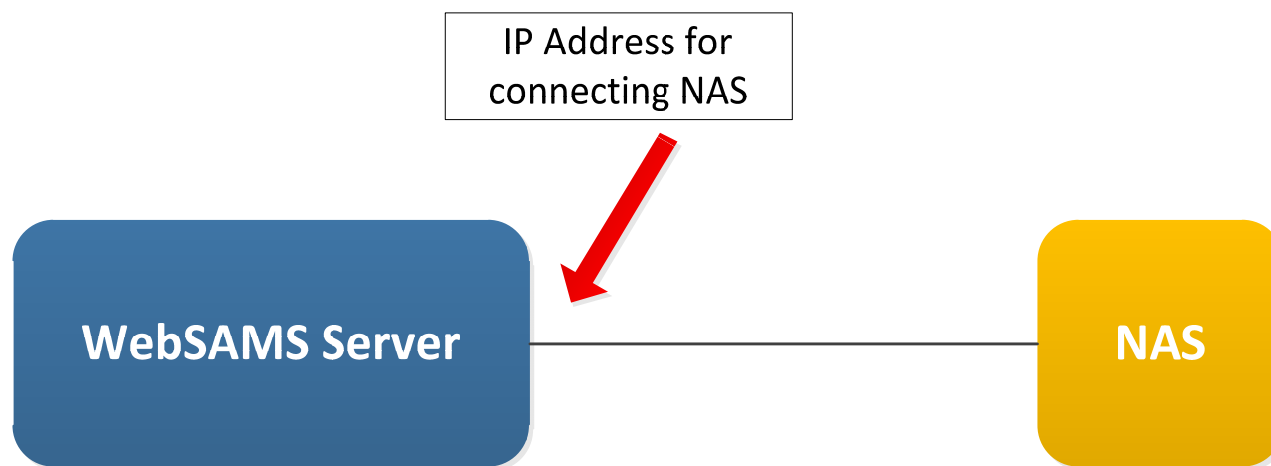
在WebSAMS路由器找到0個項目。

注意：

保安檢查功能方便學校檢查網上校管系統的基本保安設定 (詳情請參閱 "Doc24 - Network Integration Guideline For New School"、"Doc 36 - Rules for Configuration of WebSAMS Router and Internet Gateway" 及 "Doc 33 - Installation Guide for WebSAMS 3.0")。如遇技術問題，請聯絡網上校管系統求助台。其他查詢，請聯絡 貴校的學校聯絡主任。

## Reference Material (Cont'd)

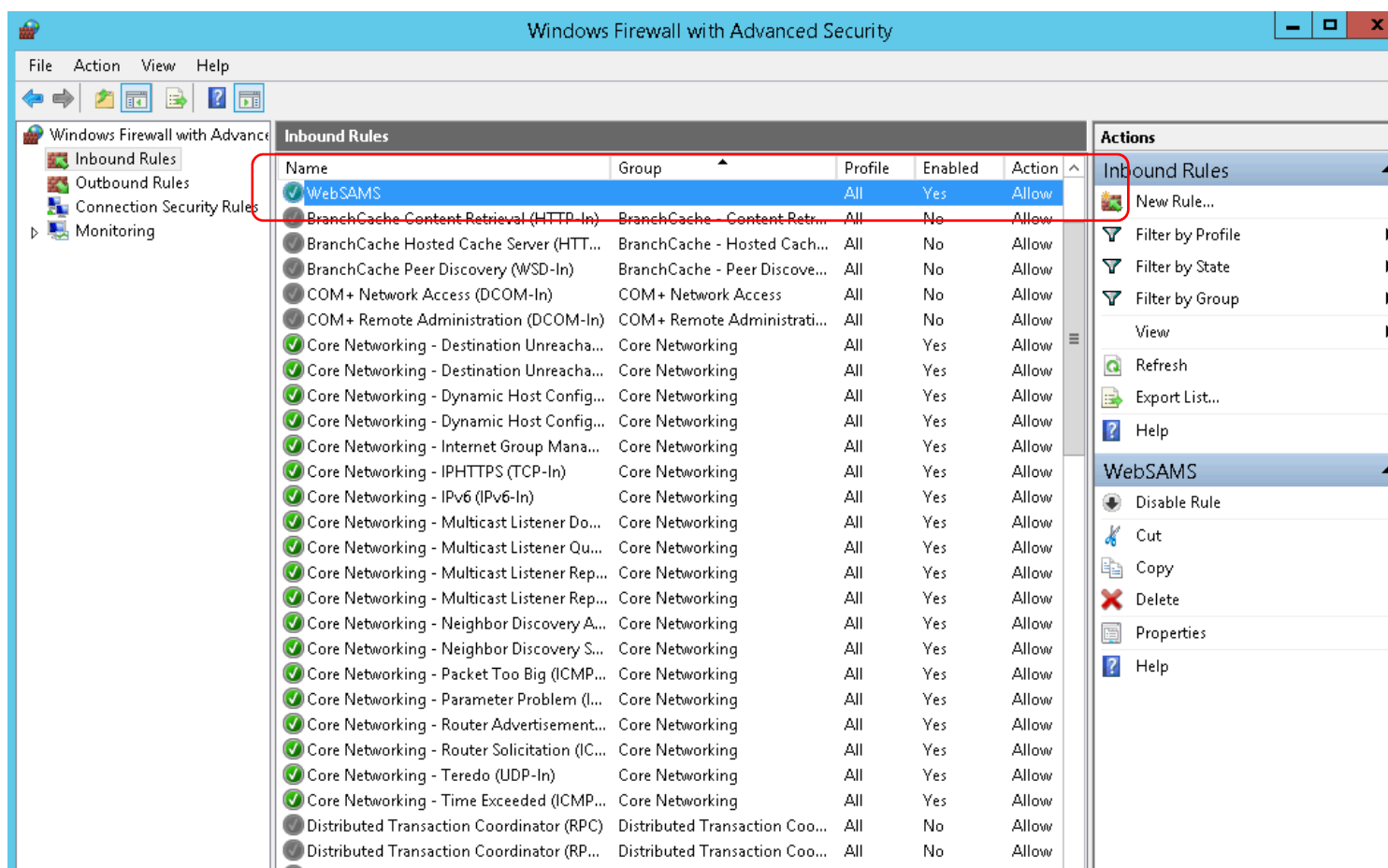
- IP Address for connecting NAS:



# Reference Material (Cont'd)

- Windows Firewall Settings:

*Control Panel > Windows Firewall > Advanced Settings*



- **WebSAMS Version Upgrade release note:**

*<http://www.websams.edb.gov.hk> > Version Upgrade for 3.0 > Major Upgrade*

- **IT Security in Schools – Recommended Practice:**

*[http://www.edb.gov.hk/attachment/en/edu-system/primary-secondary/applicable-to-primary-secondary/it-in-edu/WiFi900/IT\\_SecurityinSchools\\_RecommendedPractice\\_Aug2016.pdf](http://www.edb.gov.hk/attachment/en/edu-system/primary-secondary/applicable-to-primary-secondary/it-in-edu/WiFi900/IT_SecurityinSchools_RecommendedPractice_Aug2016.pdf)*

## Reference Material (cont'd)

---

- Regularly visit the Information Security website of HKSAR for the update information of IT security

*<http://www.infosec.gov.hk>*

- Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT)

*<https://www.hkcert.org>*

### For enquiries:

- **Technical support:**

- WebSAMS Helpdesk 3125 8510

- **Other enquiries:**

- School Liaison Officer of the WebSAMS Team

*<http://cdr.websams.edb.gov.hk/Files/Doc/WebSAMS%20School%20Liaison%20Officer%20list.xls>*

**The End**