# NonStop System Console Security Policy and Best Practices

**Technical White Paper**

**881540-001**

# Contents

## Overview

The HPE NonStop System Console (HPE NSC) is a rackmount server or a deskside workstation running the Microsoft® Windows® Server OS and containing software used to manage the HPE Integrity NonStop X and NonStop i servers. On HPE Virtualized NonStop systems, the HPE NSC software is deployed on a VM running the Windows Server OS.

Because of the console's critical role, it is important to keep its access and use tightly secured. This document describes the policies that HPE has in place and best practices that HPE recommends to help customers satisfy their security and audit requirements related to NSCs.

This document describes HPE's policies with respect to:

- HPE NSC software updates
- Customer selection and administration of antivirus and firewall software
- Customer administration of software security patches

It also covers HPE-recommended best practices with respect to:

- Securing your location
- Securing your operating system
- Securing your network

## NSC security policy

NSCs are not intended to be used as general-purpose PCs, and should not be managed as if they were. You should not install software on NSCs other than what is described below.

Physical NSCs shipped by HPE include the following installed software:

- The Windows Server OS and associated utilities such as Remote Desktop
- HPE-supplied software such as Open System Management (OSM) Low-Level Link and OSM Console Tools
- comForte MR-Win6530 (to support terminal emulation)
- Oracle Java (for various functions)
- Adobe® Acrobat® Reader (to read PDF files)

You also may install additional management software such as HPE Insight Remote Support (IRS), and HPE NonStop Essentials on the NSC.

See the NonStop Console Installer Guide for details on installation of these products.

The list of software products automatically and optionally installed on the NSC may vary in the future.

### NSC software updates

The HPE policy on NSC security software updates is as follows.

**Software developed by HPE specifically for NonStop environments**

Software developed by HPE for the NSC enables customers to manage their NonStop systems. Software used with the HPE Virtualized NonStop, HPE NonStop X, and HPE Integrity i servers is updated on a regular basis, typically two or three times a year. Where practical, HPE includes all fixes available for known security problems and any available enhancements in these release updates. An updated version of HPE NonStop Software Essentials also is always included on the HPE NSC DVD. Recent versions of NonStop Software Essentials no longer have a dependency on HPE Systems Insight Manager (SIM), so the latter is no longer delivered on a companion DVD. NonStop Cluster Essentials (NCE) does still have a dependency on SIM, but HPE recommends installing NCE on Central Management Servers (CMS) rather than on NSCs.

**Software developed by HPE specifically for Microsoft environments**

Customers may choose to install software developed by HPE for Converged Infrastructure management such as IRS or SIM on their NSCs. In that case, the customer is responsible for downloading and applying security patches in a timely manner.

**HPE management firmware and software**

NSCs include both HPE System Management Homepage (SMH) and HPE Integrated Lights Out (iLO) Server Management software to monitor and manage the NSCs themselves, depending on customer preference. Updates to the software and firmware packages are available on the Service Pack for ProLiant (SPP) solution, which is delivered as a single ISO image. Access to the SPP requires validation via the HPE Support Center, as an active warranty or HPE support agreement is required to download the SPP. Single firmware or software packages for management also are available from the HPE Support Center. You can get drivers and manuals by entering the NSC product name or number and following the link for Drivers & software.

**Software developed by third parties included on the NSC**

The versions of software developed by Microsoft or other third parties that are delivered by HPE are updated depending on the third party’s frequency of software updates. As updates or service packs become available from the software vendor, HPE updates the base software on the NSC appropriately. HPE delivers security fixes and enhancements that are part of the vendor updates by incorporating a service pack or software update into the HPE NSC software bundle. Customers are responsible for checking for and applying additional security updates as required by their corporate IT policies and local practices.

When installing a new or spare NSC or an NSC software update, customers should check its Windows version against the most current security updates from Microsoft. HPE ships NSCs with Microsoft released patches; however, Microsoft is likely to have issued security advisories, bulletins, and update roll-ups since the NSC was configured or the NSC DVD was produced.

HPE ships the NSCs with Java updates released by Oracle; however, similar considerations apply with respect to updates.

The HPE NSC software bundle also includes Apache OpenOffice, primarily for use by HPE support. Customers may update the version of Apache OpenOffice on the NSC as needed, or, if it is not used, delete it.

## Customer installation of additional software on the NSC

Installing software not approved by HPE – or different versions of approved software – on a NonStop system console is not advised in most cases. The exceptions are antivirus (AV) software and software firewalls.

HPE believes that it is important for customers to install AV software on NSCs. This includes NSCs that are not accessible from the public LAN, which should still be kept updated with antivirus software and current virus definitions on a regular basis.

HPE ships NSCs without antivirus software because there are many AV packages available for Windows, and companies often either are mandated to or prefer to install the specific AV product that is designated in their corporate standards and configure it in a prescribed manner to meet their standards and communicate with their enterprise security monitoring infrastructures. Customers usually have site licenses for one or more AV packages that cover installation on their NSCs.

HPE also recommends either enabling the Windows software firewall or installing the customer's choice of firewall.

- HPE makes no recommendations regarding the choice of one third-party product over another.
- All responsibility for use of third-party products rests with the customer.
- Customers must purchase these software packages directly from the appropriate vendor.
- HPE does not accept support calls related to the functioning of the antivirus or firewall software on the NSC.
- Customers using an antivirus or firewall package may be asked to temporarily disable the package to assist the GNSC in troubleshooting an NSC-related problem.

---

**Note**

Customers may run OSM Service Connection on other PCs; however, HPE reserves the right to not provide support for that configuration in cases where a customer cannot reproduce a problem on an NSC.

---

## Customer administration of software security patches

It may be necessary for customers to install software patches on their NSCs between scheduled software releases, especially when those patches correct security vulnerabilities. It is up to each customer to decide what to install and when. HPE's policy on handling security-related patches for the NSC is as follows:

**Software developed by HPE NonStop for the NSC**

If there is an urgent security fix, HPE notifies customers through a NonStop Hotstuff containing a description of the problem, the workaround (if any), and instructions on how to obtain and install a fix for the problem.

**Software developed by HPE specifically for Microsoft environments**

HPE recommends that customers who install HPE products such as IRS, SMH or SIM on their NSCs proactively install security patches.

**HPE firmware and management software**
If there is an urgent security fix, HPE notifies customers through Support Alerts. HPE will also notify customers who subscribe to ExpressNotice through a NonStop Hotstuff or Support Note containing a description of the problem, the workaround (if any), and instructions how to obtain and install a fix for the problem. Customers can subscribe to receive HPE alerts and NonStop notifications; see the Resources section for details.

**Software developed by Microsoft included on the NSC**
HPE installs Microsoft's monthly security patches promptly on internal NSCs, exercises basic functions, and uses the patched NSCs for its day-to-day testing and other operations. HPE recommends that customers proactively install Microsoft monthly updates on their internal NSCs.

If HPE were to find an incompatibility during testing, customers would be notified in a timely manner through a NonStop Support Note released through ExpressNotice. The note would describe the problem that had been seen and provide customers with HPE recommendations for action. These may include performing a workaround, delaying installation of a particular Microsoft update, removing a particular update, or installing a time-critical fix (TCF) to an HPE product.

HPE is aware that sometimes Microsoft withdraws software patches after they are announced and reissues corrected versions. HPE does not recommend that customers continue to run “recalled” Microsoft software on their NSCs.

If Microsoft announces a serious or destructive security problem outside the normal monthly process, HPE reserves the right to provide customers a warning and may release a Hotstuff through ExpressNotice to recommend actions that customers can take to protect their consoles. HPE reserves the right to decide whether an announced security vulnerability is serious enough to warrant this type of notification.

---

**Note**
HPE does not issue Hotstuffs for the normal monthly Microsoft patch releases.

---

**Monitoring security patches for HPE-developed software**
HPE recommends that customers register with HPE to receive HPE Security Bulletins and NonStop notifications for products of interest.

## Software developed by other third parties included on the NSC

HPE recommends that customers monitor security patch availability for third-party products such as Adobe® Reader® that are installed on the NSC. If a third-party vendor announces a serious or destructive security vulnerability outside of its normal process, HPE may choose to provide customers with a warning about their exposure on the NSC and may release a Hotstuff through ExpressNotice to recommend actions that customers can take to protect themselves. HPE reserves the right to decide whether an announced security problem is serious enough to warrant this type of notification.

---

**Note**
HPE does not issue Hotstuffs for the normal third-party vendor patch releases.

---

## NSC security best practices

In the past, NSCs usually were well isolated. They were connected only to the NonStop maintenance network (LAN), which was not connected to any public network. They sat in a physically secure environment where physical walls and locks prevented their use by the unauthorized. The only connection they had to the outside world was a modem that dialed out problems to HPE. The software on these consoles was (and still is) highly controlled and only a fully tested suite of software was allowed on it.

Current customer requirements and infrastructure have made this model much less applicable. NSCs as delivered are connected only to the maintenance LAN, but customers may choose to also connect them to corporate intranets that may in turn be connected to other networks. NonStop system maintenance functions are often performed from PCs that are not NSCs, either directly using OSM Service Connection or indirectly through Remote Desktop running on the NSC.

You need to secure your NSCs in a manner that is appropriate for your current usage model.

### Securing your location

The first step to a secure system is a system that is secure physically. Chances are that you already have excellent physical security for your NonStop systems. Locked, access-controlled data centers are the norm for such mission-critical computers. Your consoles should meet the same level of security and be treated like the vital part of your NonStop system that they are.

Details about physical security are outside the scope of this document, but consider the entire continuum of equipment that comprises your NonStop system when planning your physical security:

- HPE NonStop servers, including Cluster I/O Modules (CLIMs)
- HPE NonStop System Consoles
- The networking equipment
- Any other desktops or laptops that connect to the maintenance LAN
- Any other desktops or laptops that remotely control the NonStop System Console

Any PC, no matter how well secured by software, can have malicious software added if physical access is allowed. Remotely controlling the console with a contaminated laptop can open the door to insecurities (for example, installation of keystroke loggers.) Physical forms of access such as DVDs (other than HPE installer DVDs) or USB Memory sticks also are potential sources of malicious software and also require strict controls. HPE does not recommend specific preventive measures, but does encourage application of local security policies to govern the use of external media. The policies may include disabling drivers, restricting access, or adding physical barriers to limit media and USB port access.

### Secure your operating system

A strongly secured operating system is the basis for any secure server.

Stay up to date on operating system patches. On the second Tuesday of every month, Microsoft releases that month’s security patch rollup for Windows. It is important to stay current on these patches, which close holes in the operating system kernel and other important operating system components. There are multiple ways to push the patches to the console for installation, and you should use the method applicable to your environment. Microsoft may also release out-of-band patches that are not on the same patch release cycle.

HPE recommends that you install the monthly or out-of-band patches promptly. However, environments can vary considerably and, ultimately, assessing the risk to a particular set of NSCs of deferring security patch installation is your responsibility. If you need to consider deferring installation of critical patches on some or all NSCs, here are some factors to keep in mind for risk evaluation:

- Are any of your NSCs connected to any other Windows systems outside of your NonStop maintenance LAN? Can a virus spread to your NSCs over your intranet, or an insider take advantage of a vulnerability?
- How long would it take to recover your NSCs if they were damaged by an exploit?
- How would you manage your NonStop systems during this time?

There are a number of options for patch rollup installation, including:

- Microsoft Automatic Update downloads for NSCs connected to the Internet
- Installation by corporate workstation application management software
- Download and SFTP transfer or direct delivery via USB or other connected media.

**Automatic Updates**
If you opt to configure Windows for Automatic Updates, HPE recommends that you select the “More Options” button and configure the "Download updates for me, but let me choose when to install them" option (see the screenshot below).

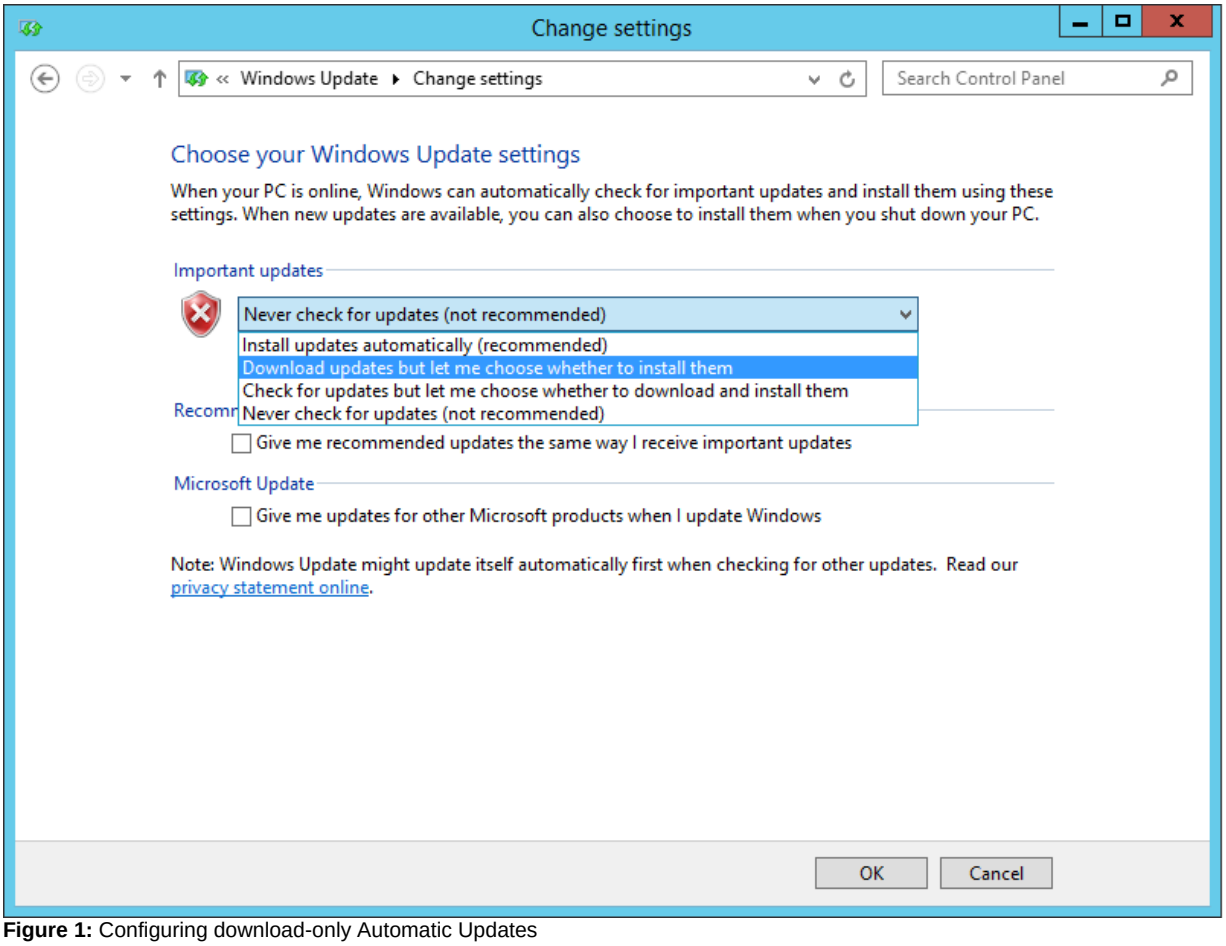

**Figure 1:** Configuring download-only Automatic Updates

This option will automatically stage the updates, allowing you to manually apply them at a convenient time. While it is rare, it is possible that a specific patch rollup will cause problems, and waiting for a short period of time (days) allows others to discover and report those problems. If you choose to either just download updates automatically or disable automatic updating entirely, make sure that you have a process in place to perform the update installation in a timely manner after the patches are released.

**Workstation application managers**
If your internal IT organization has a prescribed method for managing Windows-based workstations such as Microsoft System Management Server, you need to ensure that you have adequate controls on its use to manage NSCs. It is important to make your IT team understand that the console is not just another workstation in the network. It is a specialized tool that is an important part of keeping your NonStop system running without fail. Although HPE's policy allows you to install specific types of software not provided by HPE on your NSCs, this does not necessarily mean that

you can configure it like any other workstation in your organization. You still must tightly control the applications that are installed on the console to maintain the high level of reliability and security that you expect from your NonStop systems.

Any application manager used to manage your NSCs must be able to differentiate them from other workstations in the network and install only software that is approved for use on them. For example, typical office software such as Microsoft Office must not be installed on the console. Only operating system patches and security software updates should be managed by any such application manager. There are many ways of accomplishing this, depending on your network structure. IP addresses, subnets, and MAC addresses are examples of ways to identify and isolate consoles so you can specify different application configurations for them than are used for other Windows servers in your environment.

**Downloads**
Patches can be obtained as executable installers directly from Microsoft. Microsoft provides many ways of getting notification about what patches are available for each version of Windows. Refer to http://technet.microsoft.com/en-us/security for more information about Microsoft security for Windows. Downloading and installing the patches manually is the only solution for consoles that are kept disconnected from any public or corporate LAN. For consoles that require this level of security, HPE recommends the installation of the general OS patch rollups rather than just the security patch rollups. You will need to download the installers from the Microsoft website and move the patches to the console through some form of removable media such as a USB drive or CD-R. Be very careful to place nothing but the patches you wish to install on any removable media. Removable media is a viable vector for transporting malicious programs such as viruses. Using fresh media (such as an unused USB) is an excellent way of avoiding the import of malicious code. If possible, run an antivirus scan on the media before and immediately after copying the patch rollup to it.

## Know what is happening on your NSC

It is very important that what happens on your console is recorded. Logging and auditing are critical components to both deterring attacks on the console and identifying problems before and after they occur. Often, a security breach is made more damaging because there is no audit trail to either detect the problem or determine what went wrong and what to fix. To alter your console's security configuration, use the Local Security Settings, which is available from Start->Control Panel->Administrative Tools.

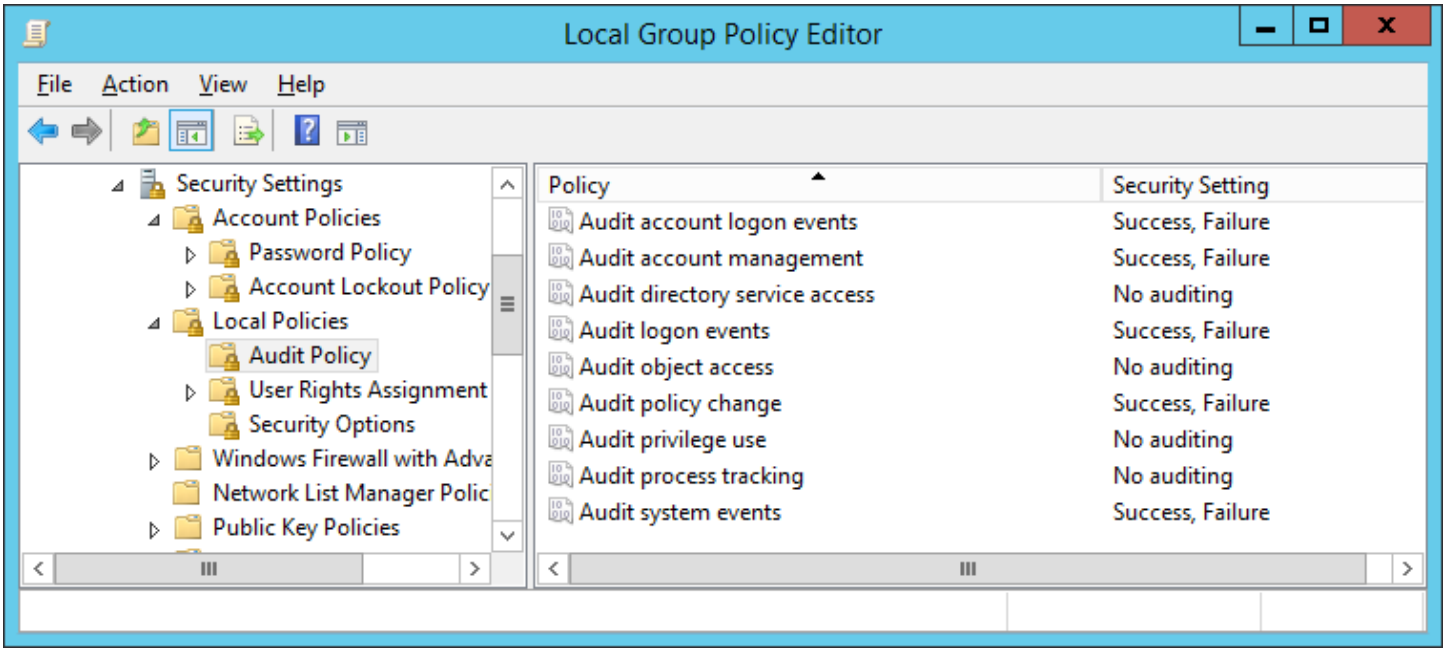


**Figure 2:** Local security settings for audit policy

The Audit Policy as set in Figure 2 lets you know who logged on to the system, who tried but failed to log on to the system, and what security changes have been made on the system and by whom. You should configure the NSC audit policy according to your corporate audit policy.

Use the Security log in the Event Viewer, which is also available from the Administrative Tools menu, to view audit. The events may also be published to management tools that can manage many systems at a time and alert you about problems as they are happening.

## Restrict access to the console

Relatively few people should require access to the NSC. Ensure that only authorized people can log onto it.

### Require individual user accounts

The NSC ships with three predefined users, each with a default password. HPE strongly recommends that you change these passwords; see the NonStop Security Hardening Guide or the NSC Installer Guide. Set unique credentials for each account, and/or modify names and access privileges as needed. Having shared accounts and passwords for the NSC with multiple users logging in as Administrator defeats individual accountability. Each user should have his or her individual NSC account, and its password should be private and not shared with coworkers.

These accounts do not need administrative rights, which are necessary only for an operator installing new software or modifying configurations of the console itself. The applications for managing the NonStop server do not need administrative rights on the console even when the user needs such rights on the NonStop system.

Some exceptions to this rule may exist, with very specialized roles using shared accounts for limited purposes. For example, there may be a designated console account for use by HPE service personnel for managing the NSC and the NonStop server. While the NSC audit would not conclusively identify who was responsible for a particular action, external logging of service personnel activity would fill in the details missing from Windows' own event log.

Another exception would be a login for monitoring the system in a lights-out environment. If a management application such as Open System Management (OSM) Service Connection stays up for long periods, with multiple people watching the same display for monitoring purposes only, it is reasonable to have a shared account for this function. However, if action needs to be taken, it is better to require that person to first log out and log back in as an individual user so that the individual user is logged as having performed the action.

When a user has left the organization or no longer needs access, be sure to revoke NSC (and NonStop system) access immediately. Having a well-defined process in place that tracks which user has access to what resources and the privileges they have on those resources and embedding this process into other processes that would change access, such as employee termination, is the best way to help ensure that revocations happens quickly and reliably.

### Require secure passwords

Ensure that each user account has a strong password. The password policy is managed through Local Security Settings.

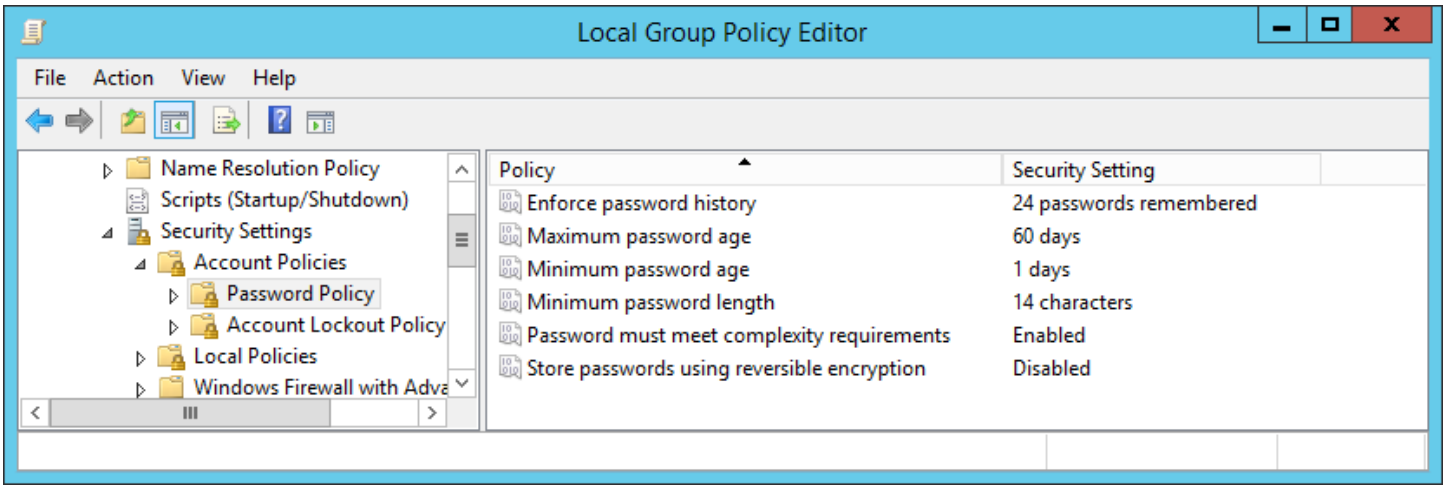

Figure 3: Local security settings for password policy

Figure 3 shows a reasonable choice of settings for NSC password security requirements. However, HPE recommends that you configure the settings to match the password settings required by your corporate policy.

**Limit account permissions**
Workstation PCs are usually configured so that any authorized network user may log in with correct network credentials. Sometimes the default permissions for such a user include local administrator rights. The NSC is not just any other workstation. Ensure that your network environment is configured so that only users that have a need to be able to use the NSC have credentials that would allow them to log onto it.

**Protect against malicious code**
Even with the best systems, malicious code may occasionally find its way onto the NSC. Malicious code could come in the form of a virus present on a USB key or it could be a worm that hikes its way across the network or intranet through an unpatched operating system vulnerability. The last line of defense against importing malware is antivirus software.

As noted above, HPE highly recommends that you run antivirus software on the console.

When running antivirus software, it is critical that you keep the software up to date. If the NSC has access to the Internet, the antivirus software should be configured for automatic updates of both the antivirus software and the virus definitions, preferably with daily or more frequent updates. Refer to the documentation provided with your antivirus software for instructions on how to configure the product for automatic updates. If your NSC does not have access to the Internet, HPE recommends that you manually download and install antivirus definition files and updates periodically to help protect against viruses being imported through physical media.

The NSC is not an email platform, and should not be used for this purpose. Only specialized, automated email is to be sent from the console. The stringent requirements of this email can be affected by email scanning. Turn off email scanning if it is an option in your antivirus software.

**Limit your exposure to attacks**
The NSC is a specialized PC that runs specialized software to perform a specific task: manage NonStop servers. Use of the NSC for a purpose other than this increases the security risk on the NSC, and by extension, to your NonStop server.

- Do not install software other than what is approved for the NSC. For example, do not install another Web browser. Internet Explorer is the only HPE-approved Web browser.
- Do not use the NSC like a workstation or office PC. Do not run Microsoft Office applications, use email, or browse the Web (if accessible) for any reason other than what is needed to manage the NonStop servers.
- Do not run any unneeded services on the console.
- Run a security analyzer, such as Microsoft Baseline Security Analyzer (technet.microsoft.com/en-us/security/cc184924.aspx), to catch flaws in your security configuration.
- Allow remote access to the NSC only through a secure network such as a VPN or secure shell (SSH).
- Do not share folders on the console. If you need to move a file from the console to another PC, share the folder on the other PC and push the file to it.

## Protect your applications

Many applications run on the NSC, and each of them could be a potential source of security issues. Perhaps the most widely run software and the most prone to security issues is the Web browser. On the NSC the Web browser is Microsoft Internet Explorer, and IE should be configured to be as well protected as possible.

**Internet Explorer**
Configure your security settings carefully. IE includes a concept called “zones.” Various IP addresses and domain names can be added to individual zones. For instance, all of the systems and devices maintained by the NSC should sit inside the “Trusted Zone.” Network nodes including the NonStop systems, the uninterruptible power supplies (UPS), the network switches, and other such devices should be here. This zone must have most items turned on or set for “Prompt.” The tools that run in this environment depend on tools such as JavaScript and Java applets to do their work.

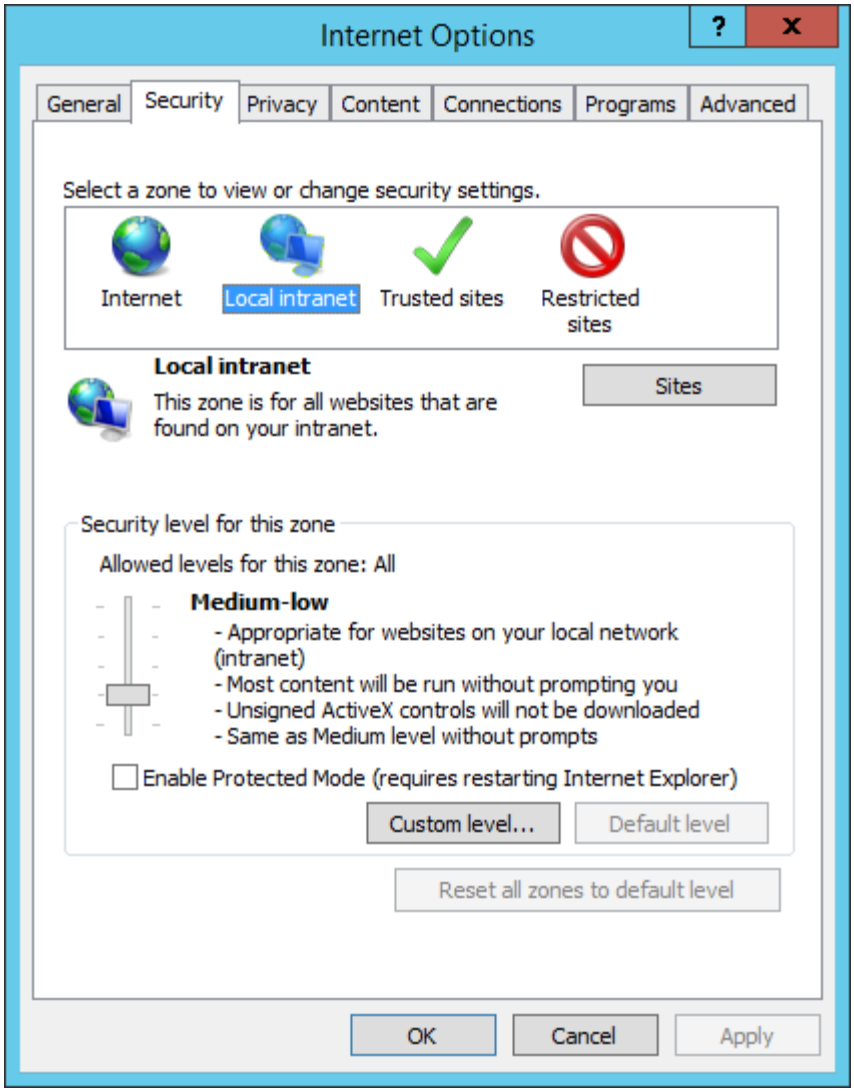


Figure 4: Internet Explorer security settings

Figure 4 shows an example of IE security settings for Local intranet. Interestingly, the zone that requires the least attention is “Restricted sites.” There is no practical way to filter out all possible bad websites. Instead, the “Internet” zone should be set up as if every site were potentially malicious. In this zone, most items should be set to “Disable” or “Prompt.” Websites that must be accessed from the NSC should be moved to the “Trusted" zone.

**Java Runtime Environment**

The Java Runtime Environment (JRE) from Oracle is an important foundation of many applications that run on the NSC. There are many versions of the JRE available from Oracle, and a product that works with one version may or may not work with another version. It may be necessary for you to have multiple versions of the JRE installed on your NSCs at a given point in time, in which case you will need to apply security updates to each of them as required.

JRE version IDs reflect major and minor revision levels and associated update levels. Changes to major and minor JRE revisions can reflect broad functionality changes, and it is entirely possible that a piece of software designed to run on Java 7 will not function correctly on Java 8. The update revision level within the version is used to identify sets of security patches and defect repairs. These updates are the ones that should be installed on the NSC. Do not replace one major or minor revision with another without verifying that you will be able to continue to run all required applications.

The JRE version can be decoded as follows, using the example of 1.8.0_121. The first part always is 1 and can be ignored. The second part is the major revision - in this case, 8, and this version of Java is referred to as Java 8. The third part is the minor revision, which changes infrequently. The last part is the update version - in this case, 121. This version of Java also may be referred to as Java 8u121.

For example, if you have applications on the NSC that require Java 7 and also Java 8, you may have 1.7.0_80 and 1.8.0_121 installed. These two versions will co-exist without conflicting with each other. Figure 5 shows an NSC with three JRE versions installed concurrently.

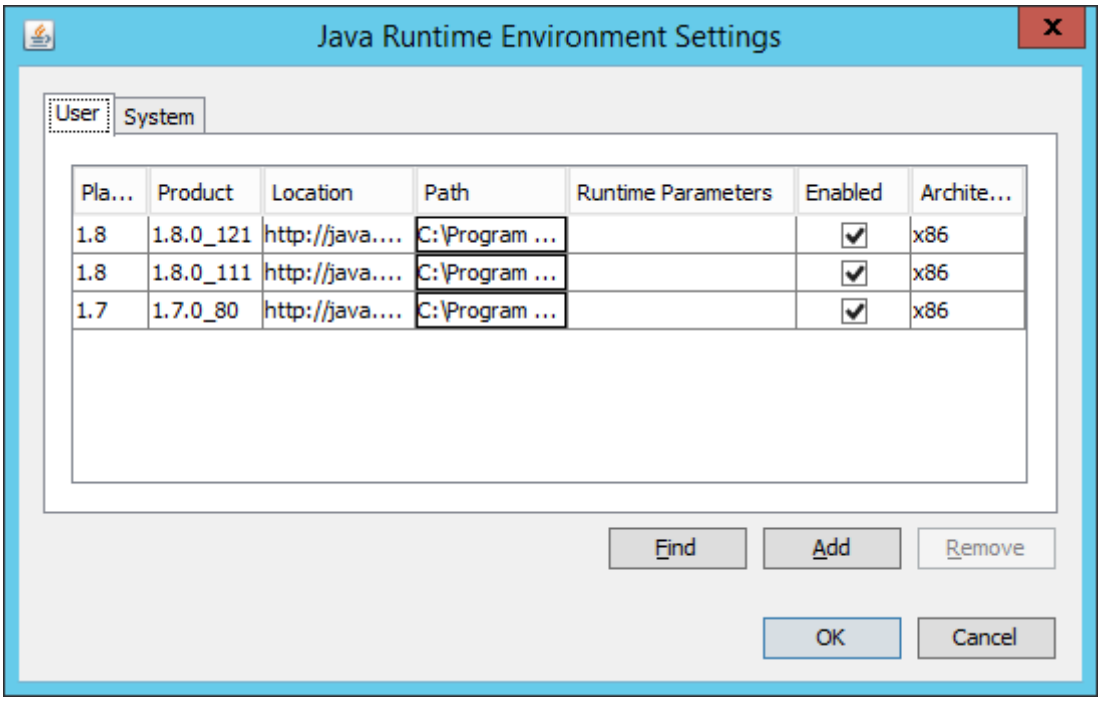


Figure 5: Java Runtime Environment settings

**Note**
If your NSCs are being managed by your corporate Windows application manager, it is important that you point out that policies that apply to normal servers do not necessarily apply to NSCs. Application of some of the more restrictive policies, such as removing old versions of Java by default or turning off DNS/DHCP/WDS/File Server, will create a situation where the NSC is unable to manage your NonStop Server.

## Secure your network

Your corporate network is the primary entry point for most security attacks. Great care should be taken to secure this entry point to the console.

### Isolate your networks

HPE recommends that your maintenance LAN be separated from your public and corporate LANs. This network, which comprises the Service Processors (SPs), Maintenance Entities (MEs) or Maintenance Entity Units (MEUs), Onboard Administrators (OAs), Integrated Lights-Out (iLOs), and other maintenance interfaces is a sensitive part of the NonStop system. The recommended way to support corporate intranet access to the console is by having two network interfaces available on the NSC as shown in Figure 6. All currently shipping NSCs come with a minimum of two NICs. Some older NSCs do not have two NICs. Contact HPE Support for assistance if you need to upgrade to two NICs on your NSCs.

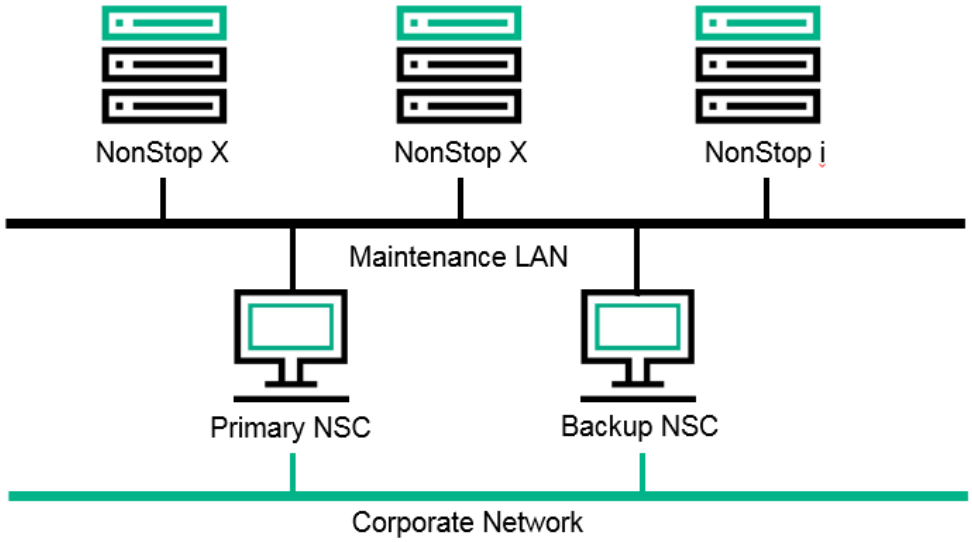


Figure 6. NSC connectivity

Figure 7 shows the Network and Sharing Center screen for an NSC with dual-network connectivity:

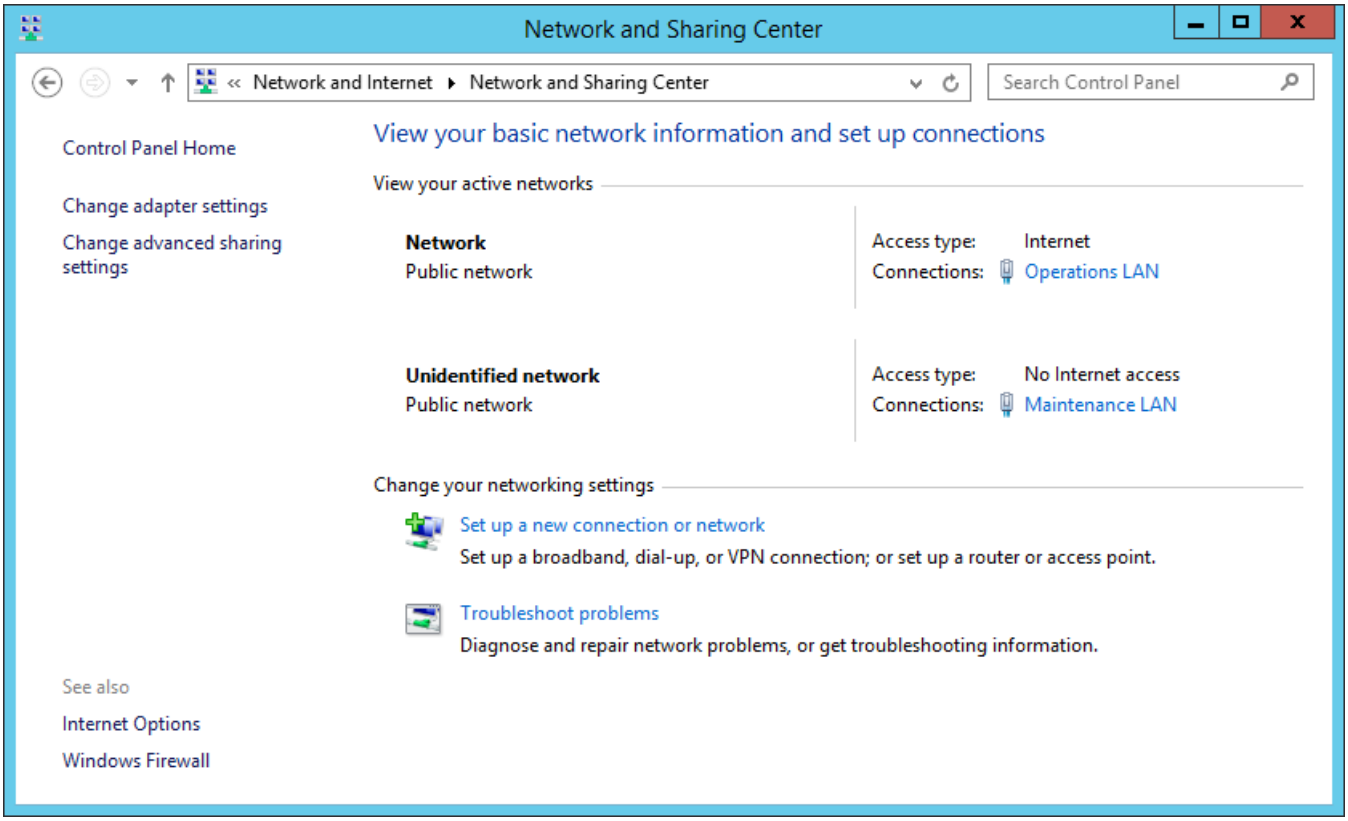


Figure 7: Maintenance LAN and Corporate LAN

If you wish to have remote access to applications that may only run on the maintenance LAN, such as OSM Low-Level Link, HPE recommends using Remote Desktop Connection to connect to the NSC. Only allow access to the console to

those users that legitimately have a need to connect remotely. To activate Remote Desktop on the console, use the System Properties dialog box available from Start->Control Panel->System.

If you don't require use of Remote Desktop, ensure that it is disabled as is shown in Figure 8.

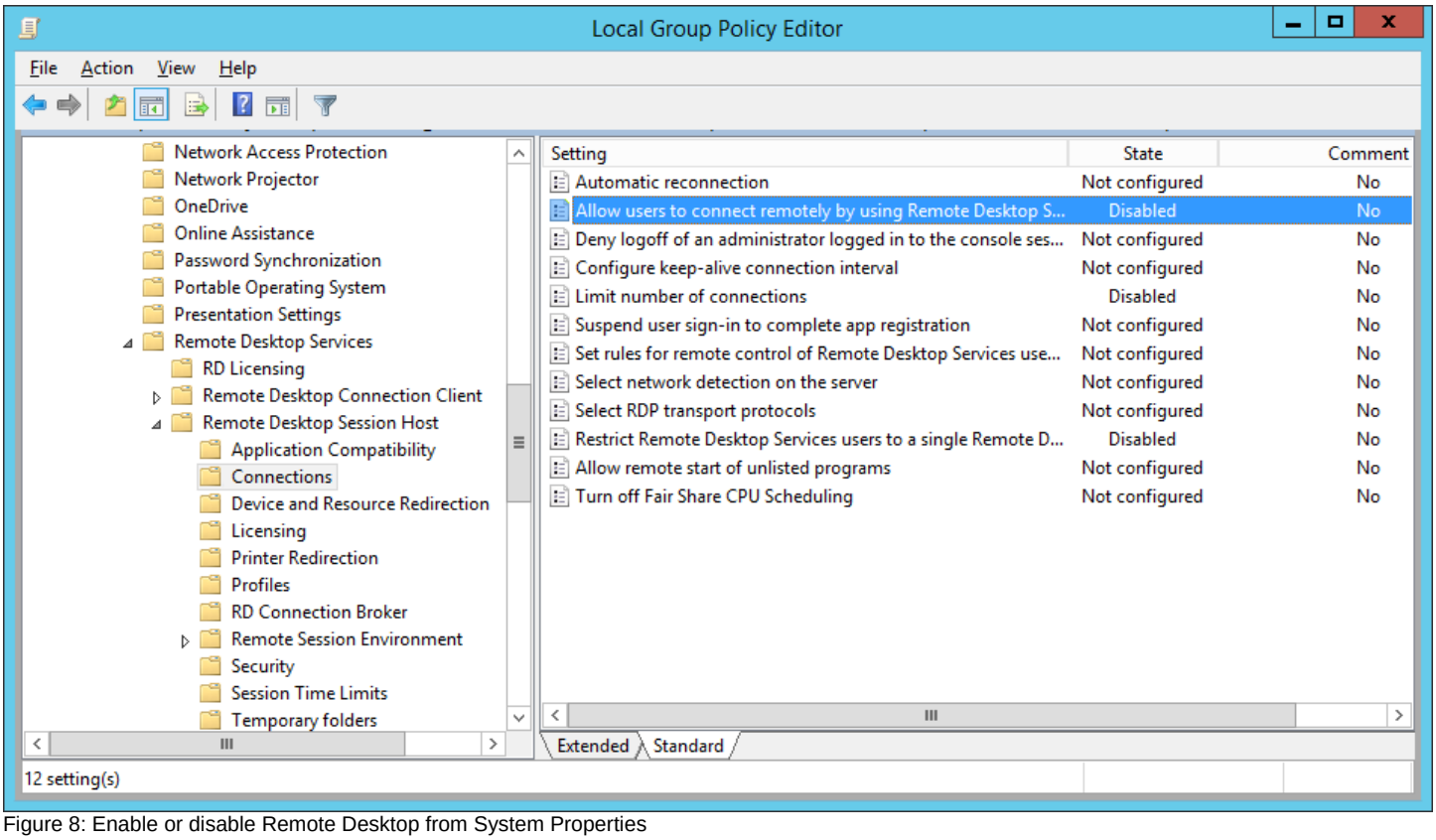

Figure 8: Enable or disable Remote Desktop from System Properties

Some manageability applications, such as OSM Service Connection and OSM Event Viewer, are certified to operate on the public LAN. Access to OSM Service Connection and OSM Event Viewer must always be present on the maintenance LAN. If you wish to also make them available on the public LAN, refer to the OSM Configuration Guide for instructions on how to configure them.

Insight Remote Support (IRS), which "dials out" problems to HPE over the Internet, has been engineered to restrict access to only the minimum that is required. See the documents on security in the IRS document collection for details on its design and configuration.

## Use a software firewall

HPE recommends that you run a software firewall on the console. This provides a last line of defense against intrusions onto the console from other workstations in your organization’s network that are already inside the protected zone within your hardware firewall.

There are many ways to install, configure, and manage a firewall installation on the console. Smaller organizations can do so with local settings on the console and manual updates and installations. Larger organizations may want a centralized security management server to maintain currency on all firewalls installed inside the organization. Either way is acceptable for the NSC.

HPE has found that the default configuration of most firewall packages works quite well for the NSC. The NSC does not require any inbound ports, except in some limited circumstances. It does require connections to a number of ports on the NonStop system.

| Port | Protocol | Notes |
|---|---|---|
| **20** | FTP | File Transfer Protocol (FTP) |
| **21** | FTP | FTP |
| **22** | SSH/SFTP | SSH for Tandem Advanced Command Language (TACL) and SSH File Transfer Protocol (SFTP) |
| **23** | Telnet | Telnet for TACL |
| **53** | DNS | Domain names lookups |
| **67** | DHCP/BOOTP | If you are running dynamic addressing |
| **69** | TFTP | Trivial FTP |
| **80** | HTTP | Many maintenance interface are Web servers on the port 80, including maintenance switches and UPSs |
| **162** | SNMP | If the console is managed with SNMP (for instance, by HPE SIM) |
| **280** | HTTP | HPE Systems Insight Manager |
| **443** | HTTPS | Some maintenance interfaces are HTTPS also |
| **630** | ONC/RPC | Low Level Link connection |
| **5988** | HTTP | Unencrypted OSM Common Information Model Object Manager (CIMOM) |
| **5989** | HTTPS | Secure Sockets Layer (SSL)-enabled OSM CIMOM |
| **9990** | HTTP | OSM Service Connection server |
| **9991** | HTTP or HTTPS | OSM Event Viewer server |
| **50000** | HTTPS | HPE Systems Insight Manager |

Table 1: Required outbound ports

There are occasions when the console is used as a server. In those cases, some ports will need to be open for incoming connections.

| Port | Protocol | Notes |
|---|---|---|
| **20** | FTP | FTP for cluster I/O module (CLIM) update |
| **21** | FTP | FTP for CLIM update |
| **22** | SSH/SFTP | If running SSH access to the NSC |
| **53** | DNS | If this console is being used as a Domain Name System (DNS) |
| **67** | DHCP/BOOTP | If this console is being used as a Dynamic Host Configuration Protocol (DHCP) server |
| **69** | TFTP | Trivial FTP for HSS |

| | | |
|---|---|---|
| **161** | SNMP | If the system is managed by SNMP |
| **162** | SNMP | If running as HPE Systems Insight Manager Central Management Server (CMS) |
| **280** | HTTP | If running as HPE Systems Insight Manager CMS |
| **3389** | RDP | If Remote Desktop is enabled |
| **2381** | HTTPS | If running System Management Homepage (SMH) |
| **7905** | HTTPS | If running as HPE Systems Insight Manager CMS, HPE Remote Support (version 7+) |
| **7906** | HTTPS | If running as HPE Systems Insight Manager CMS, HPE Remote Support |
| **50000** | HTTPS | If running as HPE Systems Insight Manager CMS |

Table 2: Inbound NSC ports

Refer to the documentation provided with your firewall software for instructions on how to set these ports.

# Resources

## NonStop manuals collection

www.hpe.com/info/nonstop-docs

- NonStop Security Hardening Guide
- NonStop System Console Installer Guide
- NonStop System Console Security Policy and Best Practices (this document)

## HPE security bulletins and product alerts

**Security bulletins (all products)**
https://www.hpe.com/us/en/services/security-vulnerability.html
**Support alerts**
Navigate to the Hewlett Packard Enterprise Support Center, select the product, and click on the link to sign up for alerts.

**NonStop Hotstuffs and Support Notes**
Register through ExpressNotice on the NonStop eServices Portal:

www.hpe.com/servers/nonstop-nep

## Other documents

www.hpe.com/info/insightremotesupport/docs

- HPE Insight Remote Support and Embedded Remote Support Security Executive Summary
- HPE Insight Remote Support 7.x Security White Paper

Learn more at
hpe.com/info/nonstop

Java is a registered trademark of Oracle and/or its affiliates

© Copyright 2017 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

This document contains confidential and/or legally privileged information. It is intended for Hewlett Packard Enterprise and Channel Partner Internal Use only. If you are not an intended recipient as identified on the front cover of this document, you are strictly prohibited from reviewing, redistributing, disseminating, or in any other way using or relying on the contents of this document.

881540-001 - June 2017

Hewlett Packard
Enterprise