

Technical White Paper

How to Secure Prinect Workflow.



Securing Prinect Workflow.

A printer's responsibility.

This is a companion document to the white paper [Preventing Ransomware](#) which will outline the more technical details in implementing some of the concepts highlighted in the first white paper. If you do not feel comfortable implementing any of these steps in your shop, please consult with an IT Professional or Heidelberg Professional Services to assist you. Please note that some of these suggestions may result in temporary downtime to facilitate a reboot so they should not be implemented during normal production hours. In addition, these suggestions are expected to be done by someone familiar with IT-related changes and issues. As such, they do not fall under the normal product support capabilities of the Heidelberg Technical Help Desk so you should not be calling in to get assistance modifying or troubleshooting your environment.

Security affects everyone in your plant – from the owner to the pressman – and is critical to the success of the printer. But security is not a revenue-generating component so investing time and money in it is often not a high priority. Commonly, most printers will only address security issues after they have experienced a specific incident. A lack of security is a real risk for printers just like any other business, and security is ultimately the responsibility of the printer. Remember that security is an ongoing task and not just a one-time activity; security is not just implemented in one place. The “eggshell theory” of relying on the company firewall to create a “hard shell” around the plant but leaving the inside of the plant unprotected is no longer enough.

To view or download all of our Technical White Papers visit: <https://news.heidelbergusa.com/whitepapers/>



Contents



How to Implement Security	4
Assigning Someone to be Responsible for Security	4
Maintaining a Change Log	4

How to Educate Employees	5
Acceptable Use Policy	5

How to Stay Secure	6
Maintaining Hardware	6
Installing the Latest Updates and Software	7
Anti-Virus Protection	7
Changing Passwords and Password Policies	8
Account Lockouts and Precautions	10
Controlling Shares	12
iDrac Accounts	14
Optional Precautions	14
Disabling Transport Security Layer	16

Final Steps	17
Tightening Your Security	17

Summary	19
----------------	-----------

How can I implement security?

Here's how you can get started:

Heidelberg's Prinect® Workflow uses an "open systems" concept that includes Dell® PowerEdge™ servers with Dell Precision/OptiPlex™ Workstations as the hardware platform and Microsoft® Windows™ as the Operating System. Securing Heidelberg's Prinect Workflow includes hardening these components along with hardening your infrastructure by following industry-accepted and vendor-recommended "Best Practices."

Security is both a science and an art: you must consider the impact on productivity and reach a balance that makes sense for your business. Too much security can make things not function as expected; not enough security can create vulnerabilities that can be exploited. It is strongly recommended that you have a current backup before beginning any changes to your production equipment and avoid haphazardly making all changes at one time. Evaluate each change individually for your plant then implement, test, and document.

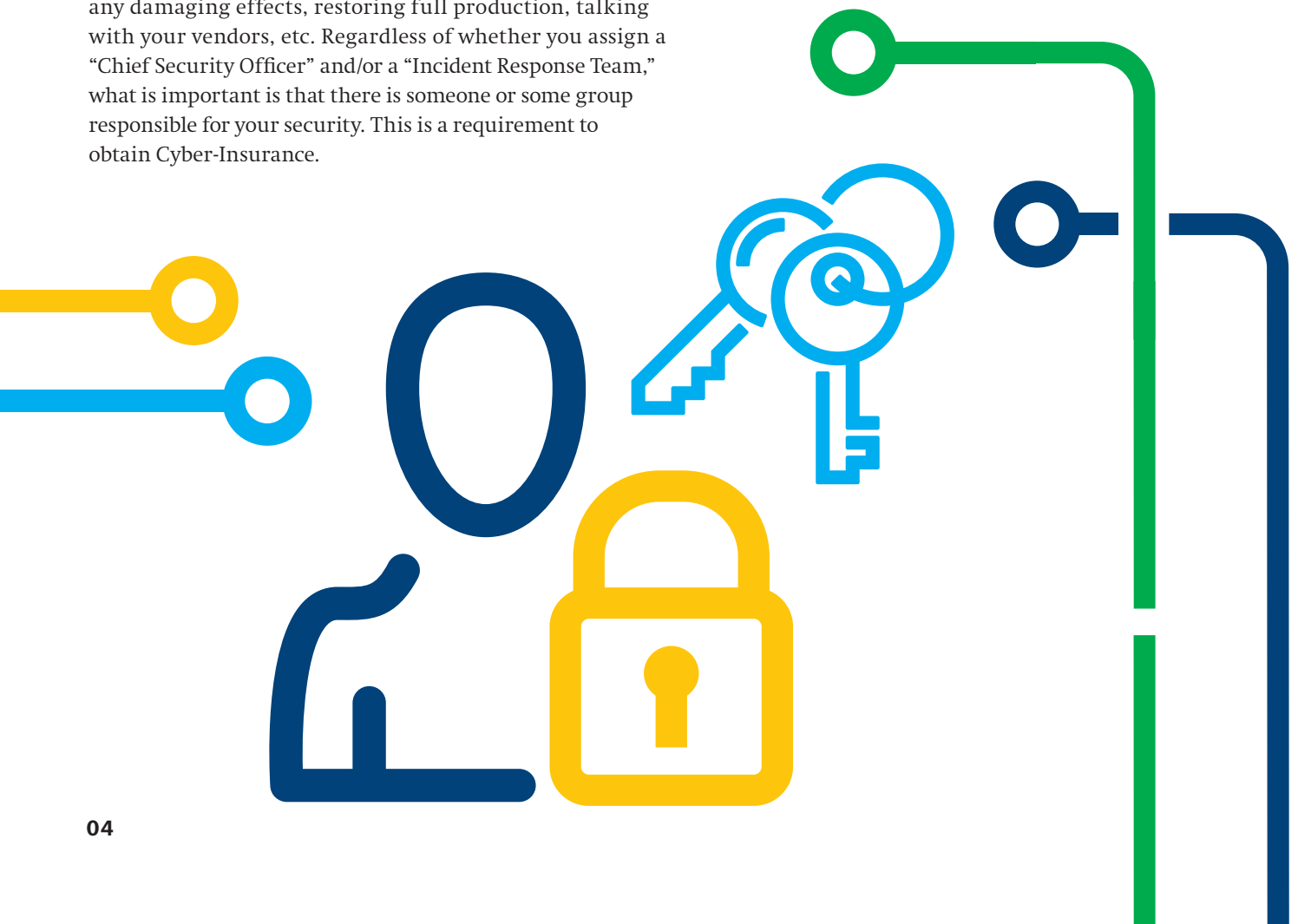
Assign Someone to be Responsible for Security

First and foremost, someone must be the "champion" of security for your business. In one sense, every individual is ultimately responsible for security; however, someone must define the standards for your plant as well as be the employees' contact when they have issues, questions or concerns.

Assign someone to be the lead for when you are experiencing a security related issue, i.e., confirming a breach, mitigating any damaging effects, restoring full production, talking with your vendors, etc. Regardless of whether you assign a "Chief Security Officer" and/or a "Incident Response Team," what is important is that there is someone or some group responsible for your security. This is a requirement to obtain Cyber-Insurance.

Maintain a Change Log

Whenever you are making changes to your infrastructure, servers or workstations, you should maintain a "change log" that documents what changes are being made, why the change is being made, who is making the change, when the change was made, etc. This will be needed if you need technical support from someone unfamiliar with your environment or if you must roll back changes due to an unexpected issue.



How can I educate my employees?

Establish an Acceptable-Use Policy:

An “Acceptable-Use Policy” is a set of documented rules and guidelines that employees in your printing plant must agree to as far as Computer Usage, Internet Usage and Email Usage. The intent is to protect both your plant and your employees from the potentially costly damages that can arise from introducing malicious software onto the Company network or jeopardizing the security and privacy of your Company's electronic communications systems. Below is an example of an “Acceptable Use Policy” but exact wording should be reviewed by your Legal Counsel to ensure you are protecting yourself.

1 Internet Usage

Company employees are expected to use the Internet responsibly and productively. Internet access is a privilege and is limited to job-related activities only – personal use is not permitted. The activities below are strictly prohibited:

- Sharing confidential material, trade secrets, or proprietary information outside of the company.
- The company may block any sites and/or downloads if they are deemed to be harmful or not productive to business.
- Social Media use outside of that required for company business.
- Sending or posting discriminatory, harrassing, or threatening messages or images.
- Downloading, copying or pirating software, music, video and/or electronic files that are copyrighted or without authorization is strictly prohibited.
- Hacking into unauthorized websites is forbidden.

The company reserves the right to monitor all inbound and outbound Internet traffic and may block any or all sites and/or downloads if they are deemed to be harmful or not productive to business.

2 Email Usage

The following is strictly prohibited:

- Emails sent via the company email system should be business related and not contain any content that is deemed to be discriminatory, vulgar, or offensive.
- Accessing personal email.
- Sending or posting solicitations, advertisements, or other content not related to business purposes or activities.

3 Computer Usage

The following is strictly prohibited:

- The installation of unwanted and/or unlicensed software not provided by the company.
- Connecting any computer devices to the company network not provided by the company without prior authorization.
- Using company computers to perpetrate any form of criminal activity.

4 Heidelberg Prinect Workflow Usage

The following is strictly prohibited:

- Use of Heidelberg Prinect Workflow components for email or web surfing.
- Connecting USB devices, inserting CD/DVD's, or connecting unauthorized Shares directly to Heidelberg Prinect servers without prior authorization.
- Installation of non-authorized hardware or software on Heidelberg Prinect servers or workstations.

→ Establishing an “Acceptable-Use Policy” for your printing plant is simply good business.

Establishing an “Acceptable-Use Policy” for your printing plant is vital to your overall security. Employees should be required to acknowledge receipt and confirm that they understand and agree to abide by the Policy.

They should also be made aware that any violation of your policy could result in disciplinary and/or legal action. This could include termination of employment, and/or employees being held personally liable for damages caused by any violations of the policy depending on the scope and frequency of the aggressions.

How can I stay secure?

1. Maintaining your hardware:

Maintain your Dell Hardware

Dell EMC highly recommends that you sign up for Driver and Firmware notifications visit <https://bit.ly/dell-drive-firmware> for information.


Dell EMC classifies updates as follows:


Urgent	Dell highly recommends applying these updates as soon as possible. These updates contain changes to improve the reliability and availability of your system.
Recommended	Dell recommends applying these updates during your next scheduled update cycle. These updates contains feature enhancements or changes that will help keep your system software current and compatible with other system modules (firmware, BIOS, drivers and software).
Optional	Dell recommends the customer review specifics about these updates to determine if they apply to your system. The update contains changes that impact only certain configurations or provide new features that may or may not apply to your environment.

When an urgent firmware or driver update is released, it is highly recommended that you update it immediately. The Dell EMC article “Update Server Firmware for Optimal Performance” explains why it is important to update Drivers and Firmware – see <https://dell.to/poweredge-update>.

The Dell EMC Server Update Utility ISO (SUU) is a local 1-to-1 utility to update BIOS, firmware, drivers and application on PowerEdge servers to the latest version. The SUU also allows comparison between the current versions installed on the server and the most up-to-date versions available. Select the components in need of updating and upon confirmation, SUU will orchestrate the deployment of the selected updates. You can download the SUU from <https://www.dell.com/support/>.

- 1 Enter your Service Tag and in the next window enter the keyword “Server Update Utility.”

Enter a Service Tag, Serial Number, Service Request, Model, or Keyword. 

What can we help you find?  or [Detect PC](#)

[Browse all products](#) [Find my Dell EMC Product](#)

- 2 Click the “Download” button, then run the executable that downloads and follow the on-screen instructions.

OVERVIEW DRIVERS & DOWNLOADS DOCUMENTATION SERVICE EVENTS PARTS & ACCESSORIES

Find a driver for your PowerEdge T640

Keyword: Operating system:

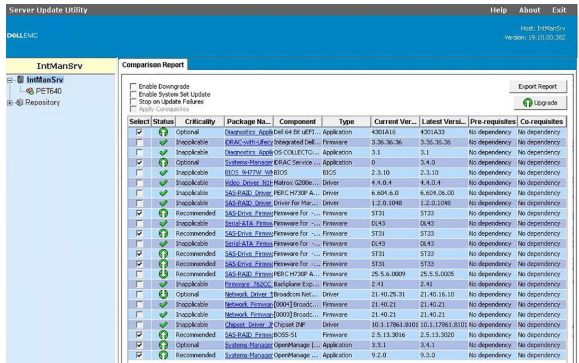
Category: Format:

☐ Show urgent downloads only

NAME	CATEGORY	RELEASE DATE
<input type="checkbox"/> DELL EMC Server Update Utility, Windows 64 bit Format, v19.10.00	Systems Management	10 Oct 2019

[Download](#)

- 3



2. Installing recent updates & software:

Install the latest Windows Update from Microsoft

Microsoft regularly releases updates for its Windows operating system. These updates include security updates to keep Windows secure as new threats and vulnerabilities are identified. At the time of the initial installation of your Prinect Server, your Heidelberg Technician should update Windows to the latest version. After that, it is the customer's responsibility to stay up-to-date moving forward. Heidelberg recommends that you configure Windows Update Settings to automatically download updates, but then you can choose whether to install them. Updates for Microsoft SQL Server must not be enabled due to possible conflicts as these will be updated through the Prinect Maintenance Center.

If you are running an older version of Microsoft Windows like Windows Server 2008R2 or Windows Server 2012R2, consider upgrading to Windows Server 2016 or Windows Server 2019. Due to security enhancements made by Microsoft, Windows Server 2016/2019 are more secure than Windows Server 2012R2 which in turn was more secure than Windows Server 2008R2.

Install the latest Heidelberg Software Updates Using the Prinect Maintenance Center

The Prinect Maintenance Center will keep your Heidelberg Prinect Workflow software up-to-date. The latest version of Prinect provides fixes to known issues and new features in addition to better security. For example, newer versions of Prinect incorporate newer versions of Apache® Tomcat™, introduce support for newer versions of Adobe® Acrobat™ and newer Operating Systems for Microsoft Windows and Apple® Macintosh™, which are inherently more secure.

3. Anti-Virus Protection:

Installing Compatible Anti-Virus

Heidelberg recommends running antivirus software on all end points in your plant, including the Prinect components. By default, Windows Defender AV is installed and functional on Windows Server 2016. In Windows Server 2016, Windows Defender AV will not disable itself if you are running another antivirus product. Using more than one antivirus product can affect the performance of Prinect and is not advised. Heidelberg does not sell or recommend any specific antivirus product or manufacturer. To avoid workflow interruption, consider configuring your virus protection application to alert, but not quarantine, potential infections. Alternately, it is also possible to exclude the folder paths listed below from virus scanning until more information is known:

Prinect Software:

C:\Program Files\Heidelberg
C:\Program Files\Common Files\Heidelberg
C:\Program Files (x86)\Heidelberg
C:\Program Files (x86)\Common Files\Heidelberg
C:\Backup Commands

Location of Data and Configuration Files:

%ProgramData%\Heidelberg
%HD_STD_USERDATA%\PTConfig
%HD_STD_USERDATA%\Hotfixes

In addition, Microsoft has the following recommendations:

- <https://bit.ly/virus-scanning-recommendation>

and for Microsoft SQL Server:

- <https://bit.ly/choosing-antivirus>



4. Changing passwords & enforcing password policies:

Change the Default Password

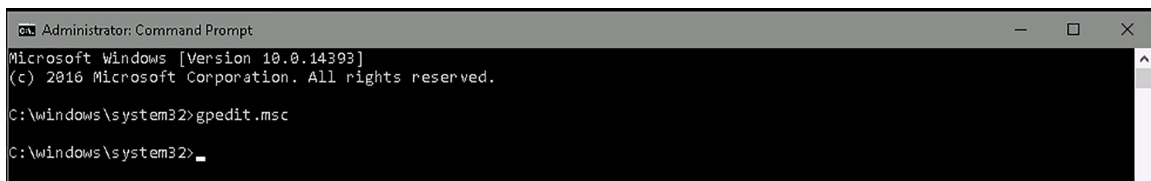
For the most part, all computer products ship from the manufacturer with a default password. It is strongly recommended that you change the password immediately upon starting up the new computer. If you don't change the password, then anyone with access to your systems can change its settings and potentially lock you out.

Prinect is no different than any other computer product in this regard. So, "Best Practice" is to change the default password for the Prinect user and the administrative account for both the workflow servers and computer. It is also recommended that you change passwords for all your infrastructure equipment as well at the time of deployment and software installation.

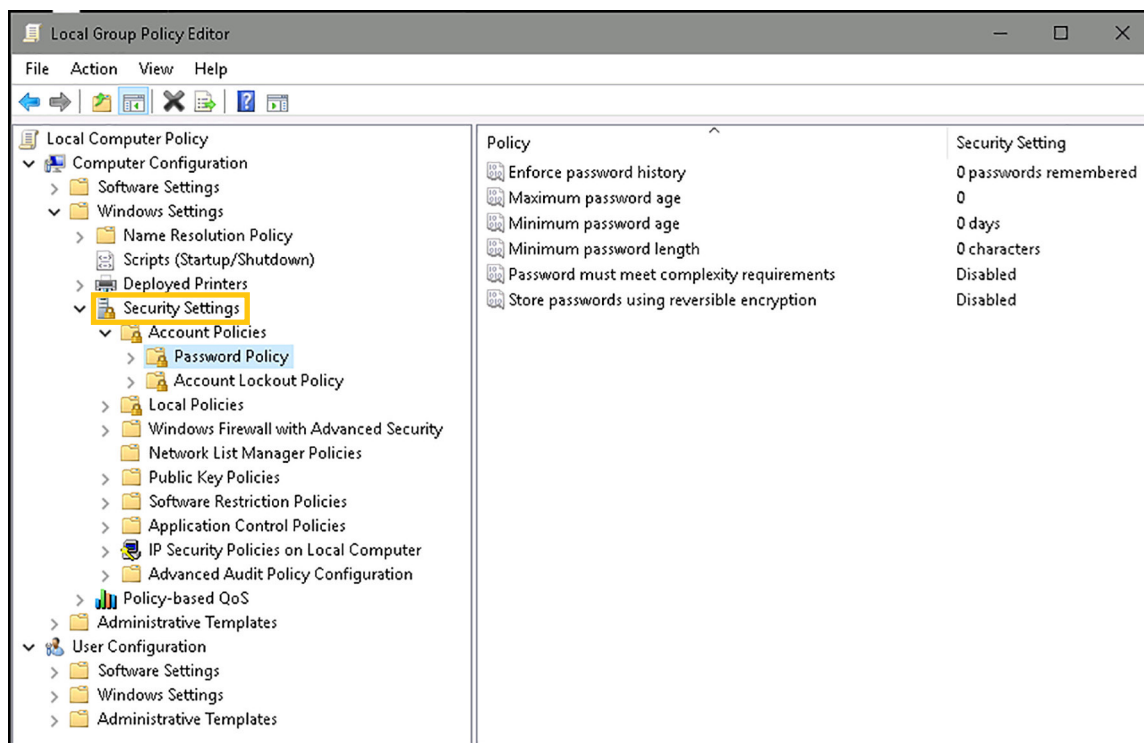
Set a Password Policy

Heidelberg Prinect servers use the Microsoft defaults for Windows. The actual settings should be defined by the individual printers that use the workflow and conform to your "Shop Standards." To set this, use the following procedure:

- 1 Open the Group Policy Management Editor by running the Command Prompt as "Administrator" and entering the command **gpedit.msc**



- 2 Open Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy



- **Enforce Password History:** This is the policy that defines how many times a user must wait before they can re-use the same password. For example, if this is set to 4, once a user sets their password to “Pa\$\$w0rd” the user won’t be able to change their password to that again until after they have changed their password 4 times. [Recommended PCI-DSSS Standard:](#) A user’s new passwords cannot be the same as the 4 previously used passwords.

- **Maximum Password Age:** This is the policy that defines the period of time in days that a password can be used before the system requires the user to change it. You can set passwords to expire after a number of days from 1 to 999, or leave it set to 0 (which is the Windows Server 2016 default), and it will never expire. If you set this to a value from 1 and 999 days, the corresponding minimum password age must be less than the maximum password age.

Please note that if this policy is enabled, it can present issues with Prinect versions prior to Prinect 2016 but has since been changed with the introduction of the Prinect Supervisor. With newer versions, you must still follow the Heidelberg guidelines for changing “Prinect” user password. It would require a change of the Prinect password, which means the services that use the Prinect account will fail to start. While Cockpit users can be configured to use the OS login, a couple of services that use the Prinect account will not start until they are updated with the new password.

Nowadays, it is considered better to have a strong password with 12 characters or more without changing it every 90 days. While it is always a good idea to change your password from time to time, it could also cause users to choose a simple password with a counting part within the password (xxxxxA, xxxxxB, ...) or writing down their password nearby the computer. [Recommended PCI-DSSS Standard:](#) Users should change their passwords every 90 days.

- **Minimum Password Age:** This is the policy that defines how long a user must use a new password after they have changed it. If this is not configured, the user can change their password several times quickly until they exceed the “maximum password age,” so they can once again use old favorite password. If you set the minimum password age, this is not possible.
- **Minimum Password Length:** This is the policy that defines the minimum number of characters that a user’s password must contain. You can set a value of between 1 and 14 characters or set the number of characters to 0 so no password is require. [Recommended PCI-DSSS Standard:](#) A password should be at least 7 characters.

Password Must Meet Complexity Requirements: This policy decides if passwords must follow these minimum requirements:

- Be at least six characters in length
- Contain characters from three of the following four categories
- English uppercase letters (A through Z)
- English lowercase letters (a through z)
- Base 10 digit (0 through 9)
- Non-alphabetic characters (!@#%&*)

Please Note: Heidelberg does not recommend enabling the “Password Must Meet Complexity Requirements” setting. In particular the Heidelberg Common Database does not allow the following characters in the password so these should not be used: &|<> ^=,; and BLANK (word space).

Do not store passwords using reversible encryption – this is the default. This policy provides support for applications that use protocols that require knowledge of the user’s password for authentication purposes. This policy should never be enabled on a Prinect server.

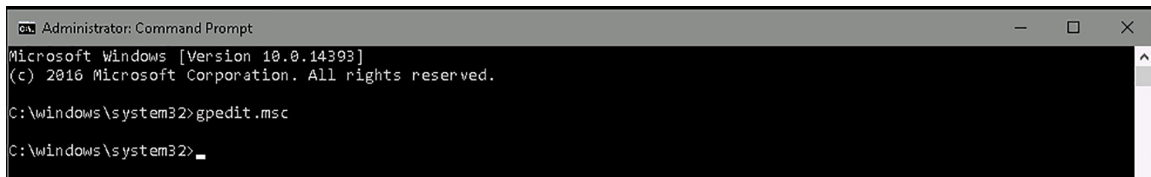
With Prinect, you must set your Prinect user accounts to use “Password for OS Login” in the Cockpit Administration.

5. Account lockouts & precautions:

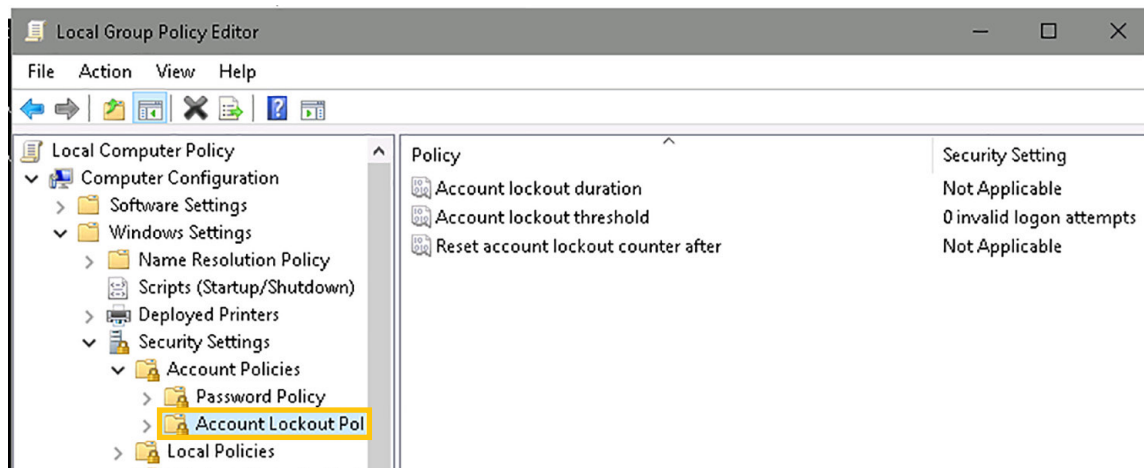
Configure Account Lockout Policies

Heidelberg Prinect servers use the Microsoft Windows default. These are defined by the individual printers that use the Workflow. To set this, use the following procedure:

- 1 Open the Group Policy Management Editor by running the Command Prompt as “Administrator” and entering the command **gpedit.msc**



- 2 Open Computer Configuration > Windows Settings > Security Settings > Account Policies > Account Lockout Policies



- **Account Lockout Duration:** This policy defines the number of minutes a locked-out account remains locked out before automatically becoming unlocked. The available range is from 0 to 99,999 minutes. If you set the account lockout duration to 0, the account will be locked out until an administrator explicitly unlocks it. If an account lockout threshold is defined, the account lockout duration must be greater than or equal to the reset time.

Typically, when you configure an account lockout threshold those two options can be configured. Otherwise, it's not possible to configure account lockout duration with lockout counter after. [Recommended PCI-DSS Standard:](#) An account must remain locked for a minimum of 30 minutes or until the “Administrator” enables the User ID.

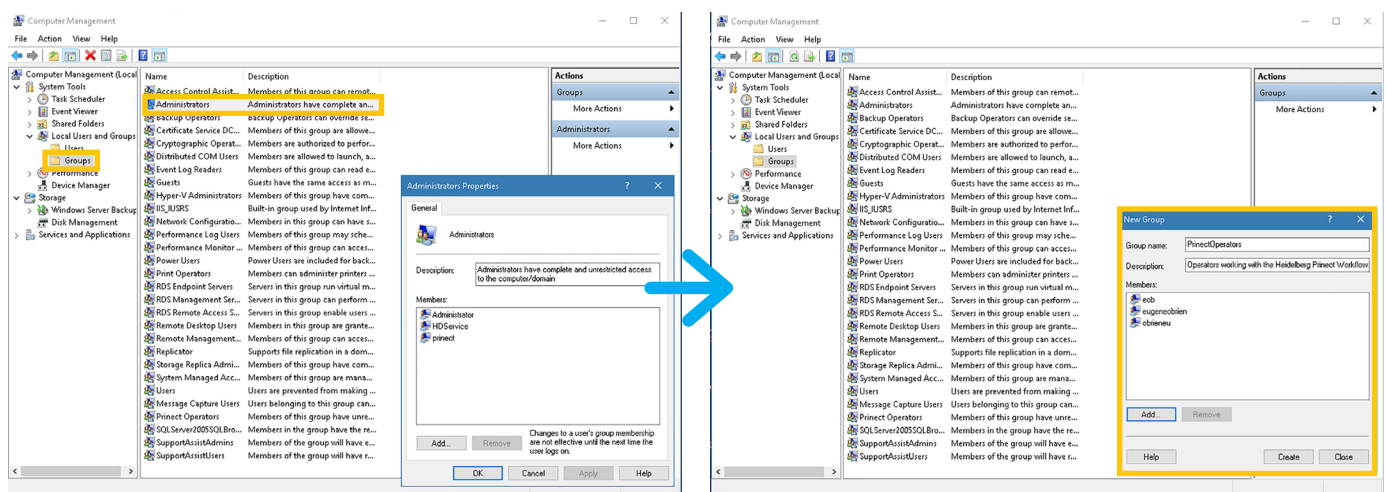
- **Account Lockout Threshold:** This policy defines the number of failed log-on attempts that causes a user account to be locked out. A locked-out account cannot be used until it is reset by an administrator or until the lockout duration for the account has expired. You can set a value between 0 and 999 failed login attempts. If you set the value to 0, the account will never be locked out. [Recommended PCI-DSS Standard:](#) A user account should be locked out after 6 failed log-in attempts. In this case, the user can only enter the password six times.

- **Reset Account Lockout Counter After:** This policy defines the number of minutes that must elapse after a failed log-on attempt before the failed log-on attempt counter is reset to zero. The available range is 1 to 99,999 minutes. If an account lockout threshold is defined, this reset time must be less than or equal to the account lockout duration. Recommended PCI-DSSS Standard: An account must remain locked for a minimum of 30 minutes or until the “Administrator” enables the User ID.

This also requires that you must set your Princt user accounts to use “Password for OS Login” in the Cockpit Administration for it to work.

- **Limit Users from the Administrators Group in All Princt Services:**
 1. Log in as an “Administrator” and open “Computer Management.”
 2. Expand “Local Users and Groups.”
 3. Under “Groups” double-click the “Administrators” and make it as empty as possible.

The recommended configuration would be as shows in the screenshots below:



Step 1: Above is for a Workgroup Server. When joined to a Domain Server, you would have four entries: Administrator, Domain/Domain Admins, Domain/princt and HDService.

Step 2: Create a new group called “Princt Operators” on each Princt Workflow Server, and add all those Windows users except the “Princt” user – that will need to be added with the Princt system into this new group/these new groups.



Note that as of Princt version 2019, this group is automatically added by the Princt Software Installer to the Princt Production Manager Server and the Princt Portal Server. But you have to add this group manually to other servers such as the Princt Data Center, Renderer, Shooter 2, etc. Any new Princt Cockpit user is automatically added to this “Princt Operators” group as long as the checkbox “Password for OS Login” is checked. So this makes adding the “Princt” user to the NTFS permissions obsolete. Please note that this applies only to the PTConfig, PTDocs and PTJobs shares. It must be manually configured to any other shares.

When joined to a Domain, you should create the “Princt Operators” group in the Microsoft Active Directory, i.e., your Domain server.

6. Controlling Shares:

Secure Any Shares

Shares on a Windows server are secured by the combined Share permissions and NTFS permissions. Even a non-Windows system must use a compatible client protocol to connect and use these shares, so it does not bypass Share and NTFS security. NTFS permissions secure the file system, whether the user is local or remote. Share permissions specify what remote access is granted. File shares use both technologies because they share resources on the file system for a remote user.

Microsoft's recommendations for sharing permissions on Shares is to set to "Full Control for Everyone" and control of access rights through NTFS rights. Control over the NTFS folder permissions allows much more granular settings, and the actual access rights that result from the sharing of Share and Folder rights are the same for Share users, local users, and users connected through Remote Desktop, if the "Share Everyone" is set up with "Full Control."

There are two possibilities to consider: Shares created by Heidelberg and Shares you (or some other program) create. Prinect Production Manager has several default Shares created by the Deployment Utility and the Installer Program.

Computer Management

FileActionViewHelp

Computer Management (Local)

System Tools

Task Scheduler

Event Viewer

Shared Folders

Shares

Sessions

Open Files

Local Users and Groups

Performance

Device Manager

Storage

Windows Server Backup

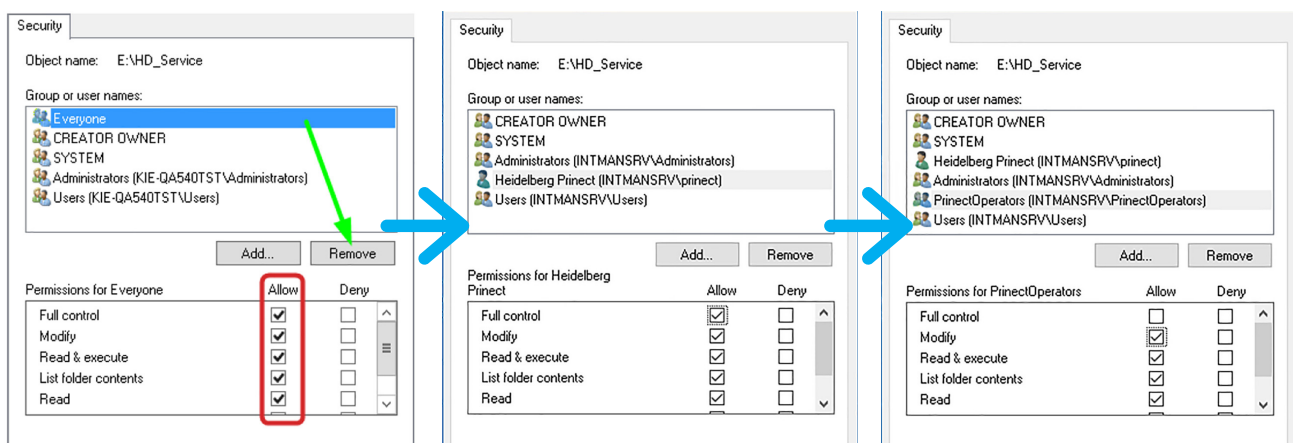
Disk Management

Services and Applications

Share Name	Folder Path	Type	# Client Connections	Actions
10-GbE Test	E:\10-GbE Test	Windows	0	<div>Shares</div> <div>More Actions</div>
ADMIN\$	C:\windows	Windows	0	
C\$	C:\	Windows	0	
CPProData\$	C:\ProgramData\Heidelberg\Color Proof Pro	Windows	0	
D\$	D:\	Windows	0	
E\$	E\	Windows	0	
HD_Service	e:\HD_Service	Windows	2	
HEIDB	\\?\GLOBALROOT\Device\RsFx0503\<localmachine>\HEIDB	Windows	0	
IPC\$		Windows	0	
Prinect_PTSupport\$	C:\Program Files (x86)\Heidelberg\Prinect Workflow\PTSupport	Windows	0	
Prinect_PTSupport64\$	C:\Program Files\Heidelberg\Prinect Workflow\PTSupport	Windows	0	
PTConfig	E:\PTConfig	Windows	3	
PTDocs	E:\PTDocs	Windows	0	
PTJobs	E:\PTJobs	Windows	0	
PTTransfer	E:\PTTransfer	Windows	0	
SQLserverLog	E:\SQLDATA\MSSQL14.HEIDB\MSSQL\Log	Windows	0	

The current recommendation is to set NTFS permissions for "Everyone" to "Read/Execute" and "PrinectOperators" to "Modify" for the primary Prinect shares. For Prinect, the Share does not require "Full Control" for the "Everyone" group. Don't forget the "Hidden Shares" – where names end with a Dollar Sign (\$).

Make sure to remove the Everyone Group from these Shares and not just remove the checkmarks but click on "Remove." Then, add the "Prinect" user and "PrinectOperators" Group to these shares with the following permissions:



The following steps illustrate the process of securing shares by removing the 'Everyone' group and adding specific Prinect users and groups:

- Initial State:** The 'Security' tab for the share 'E:\HD_Service' shows the 'Group or user names' list with 'Everyone' selected. The 'Permissions for Everyone' table shows 'Full control' and 'Modify' checked under the 'Allow' column.
- Removing 'Everyone':** The 'Remove' button is clicked, and 'Everyone' is removed from the list. The 'Permissions for Heidelberg Prinect' table shows 'Full control' and 'Modify' checked under the 'Allow' column.
- Adding Prinect Users:** The 'Add...' button is clicked, and 'PrinectOperators' and 'Users (INTMANSRV\Users)' are added to the list. The 'Permissions for PrinectOperators' table shows 'Full control' and 'Modify' checked under the 'Allow' column.

Disable Microsoft Administrative Shares

By default, Microsoft Windows automatically creates special hidden administrative shares that administrators, programs, and services can use to manage the computer environment or network. These special shared resources are not visible in Windows Explorer or in “My Computer.” However, you can view them by using the “Shared Folders” tool in “Computer Management.” Depending on the configuration of your computer, some or all of the following special shared resources may be listed in the “Shares” folder in “Shared Folders:”

- **DriveLetter\$:** This is a shared root partition or volume. Shared root partitions and volumes are displayed as the drive letter name appended with the dollar sign (\$). For example, when drive letters C and D are shared, they are displayed as C\$ and D\$.
- **ADMIN\$:** Used during remote administration of a computer.
- **IPC\$:** Shares the named pipes that you must have for communication between programs. This resource cannot be deleted.
- **PRINT\$:** Used during the remote administration of printers.
- **FAX\$:** Shared folder on a server that is used by fax clients during fax transmission.

Microsoft recommends that you do not modify these special shared resources; however, attacks via the “Administrative Shares” are well documented (see <https://bit.ly/mitre-techniques>). Princt does not use these “Administrative Shares” but if you want to remove the special shared resources and prevent them from being created automatically, you can do this by editing the registry. You must ensure that no other programs require them to work, for example, many PC Management Tools use these.



7. iDrac Accounts:

Secure the Default iDrac Account

The iDRAC is the Integrated Dell Remote Access Controller designed to make server administrators more productive and improve the overall availability of Dell servers. It is important to change the default password or anyone will be able to access the server and make changes using default credentials.

When you launch the iDRAC GUI Launcher, it will ask for a User and Password to login. The default username is **root** and the default password is **calvin**. This should be changed to a different password. It does not force you to, but it is strongly recommended that you do change it (and make record of what you change it to).

Consider iDrac Enterprise

All Dell PowerEdge Servers sold by Heidelberg were shipped with iDRAC Express – newer servers ship with iDRAC Enterprise.

If you have iDRAC Express, you can add an iDRAC Enterprise License. iDRAC Enterprise offers System Lockdown mode, which helps prevent unintended changes after a system is installed and configured. This can help protect the system from unintentional or malicious changes. Lockdown mode is applicable to both configuration and firmware updates. When the system is locked down, any attempt to change the system hardware configuration like BIOS and Firmware is blocked. If any attempts are made to change the critical system settings, an error message is displayed. So, you may want to consider purchasing upgrade licenses for any servers running iDRAC Express as an added protection.

8. Optional precautions:

Disable Remote Desktop Connections

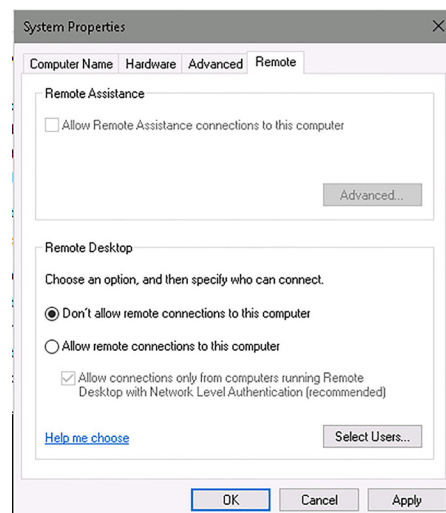
By default, Microsoft enables Remote Desktop Connections to Windows servers, so anyone that requires access within your plant does not have to be in front of the console. This may be desired depending on the size of your plant and the physical location of the Princt servers as well as the policies defined for your plant.

When enabled, this will often be flagged by “Vulnerability Scanners” because Microsoft uses a self-signed SSL Certificate for encryption. An alternative is to purchase and install an SSL Certificate from a “Certificate Authority” for Remote Desktop. You must consider the potential impact of this in your plant and minimize disruptions.

For Heidelberg Princt, Remote Desktop is not required for Princt to run, and Heidelberg does not use TCP Port 3389 that RDP uses. Occasionally, Help Desk Support Personnel may use Remote Desktop during a Heidelberg Assist session to access this server from another workstation or server where a Heidelberg Assist session was already initiated. Thus, the Heidelberg Assist session will always have to be initiated at the Princt Server, or the setting will have to be enabled temporarily. Risk is low and the effect could be undone.

Steps to Disable Remote Desktop Connections:

- 1 Open the “System Control Panel”
- 2 Choose “Advanced Systems Settings”
- 3 Select the “Remote” tab
- 4 Click the “Radio” button for “Don't Allow Remote Connections to this Computer”



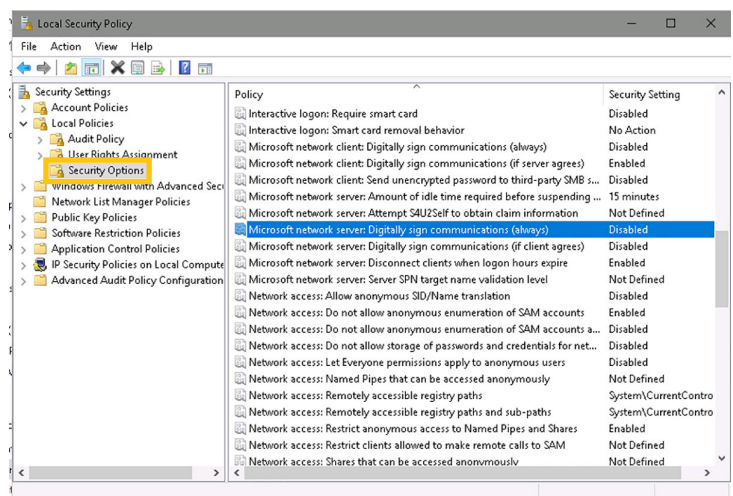


Enable SMB Signing

SMB (Server Message Block) is the file protocol most commonly used by Windows Server. SMB Signing is a feature through which communications using SMB can be digitally signed at the packet level. Digitally signing the packets enables the recipient of the packets to confirm their point of origination and their authenticity. By enabling SMB signing, all clients and servers connecting must also have SMB signing enabled or they will not be able to establish connection. In addition, there could be some negative performance impact. You must consider the potential impact of this in your plant and minimize disruption.

Steps to Enabling SMB Signing:

- 1 Open the “Administrative Tools Control Panel”
- 2 Open the “Local Security Policy Tool”
- 3 Click on “Local Policies”
- 4 Click on “Security Options”
- 5 Right-click the policy “Microsoft Network Server: Digitally Sign Communications (always)” and select “Properties”
- 6 Click the “Enable Radio” button
- 7 Confirm



9. Disabling Transport Security Layer:

Disabling TLS Versions 1.0 and 1.1

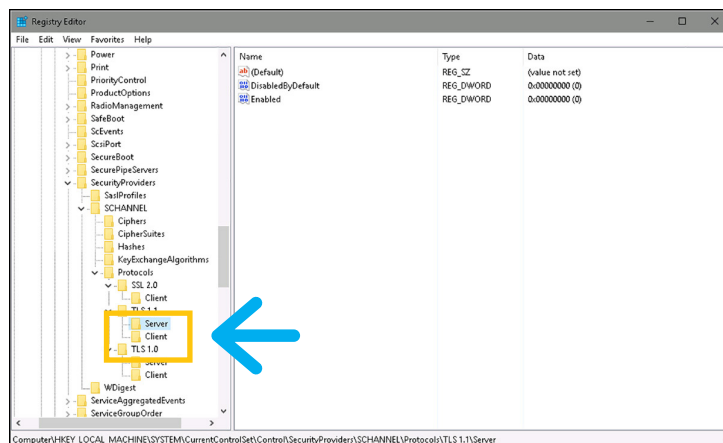
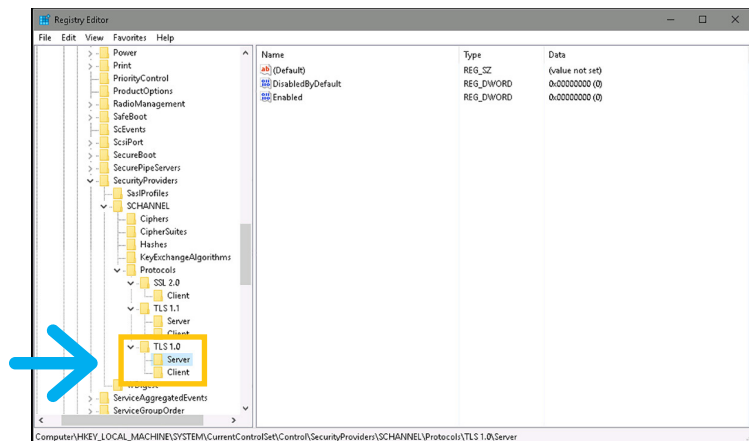
TLS (Transport Security Layer) is an IETF (Internet Engineering Task Force) standard for a cryptographic protocol that provides end-to-end network communication security to prevent eavesdropping, tampering and message forgery. It is widely used for Internet communication. Vulnerability Scanners will often flag TLS 1.0 (RFC 2246 from 1999) and TLS 1.1 (RFC 4346 from 2006) because they have been linked to Triple-DES, SWEET32, Birthday and BEAST attacks. The latest version of TLS is Version 1.3, and it is recommended for clients to implement this; however, you must consider the potential impact of this in your plant and minimize disruptions. This requires using Browsers that support it and that it is implemented in the website.

Prinect does not require the TLS (Transport Layer Security) protocol 1.0 or 1.1, so you can disable these from a Heidelberg perspective. TLS 1.2 is used by the Prinect Maintenance Center therefore, should not be disabled. TLS is an encryption cipher built into Microsoft Windows and turned on by default. The problem with disabling it is that if you use Microsoft Internet Explorer (which many still do), versions 7 through 10 do not support higher versions of TLS. If a company uses one of those browser versions, there could be an adverse effect on those companies if we disable it.

Steps to Disable TLS 1.0 for Client & Server:

- 1 Open "Regedit" (Run as Administrator)
- 2 Add the following keys:

```
[HKEY_LOCAL_MACHINE\SYSTEM\
CurrentControlSet\Control\
SecurityProviders\S CHANNEL\
Protocols\TLS 1.0\Server]
```



Steps to Disable TLS 1.1 for Client & Server:

- 1 Open "Regedit" (Run as Administrator)
- 2 Add the following keys:

```
[HKEY_LOCAL_MACHINE\SYSTEM\
CurrentControlSet\Control\
SecurityProviders\S CHANNEL\
Protocols\TLS 1.1\Server]
```


Final Steps.

Tightening your security:

Consider a Domain

Princt will work in either a workgroup environment or a domain environment (like Microsoft's Active Directory) – just not a mixed environment. With a workgroup, you must manage all security settings at each device across your network. This could make your environment less secure because you are more likely to miss something. With a domain, all security settings can be managed centrally, effectively removing the likelihood that a device will be missed. Of course, you must harden the domain servers (see <https://bit.ly/security-best-practices>).

Please Note: A domain requires investment for the hardware and requires some skills to administrate.

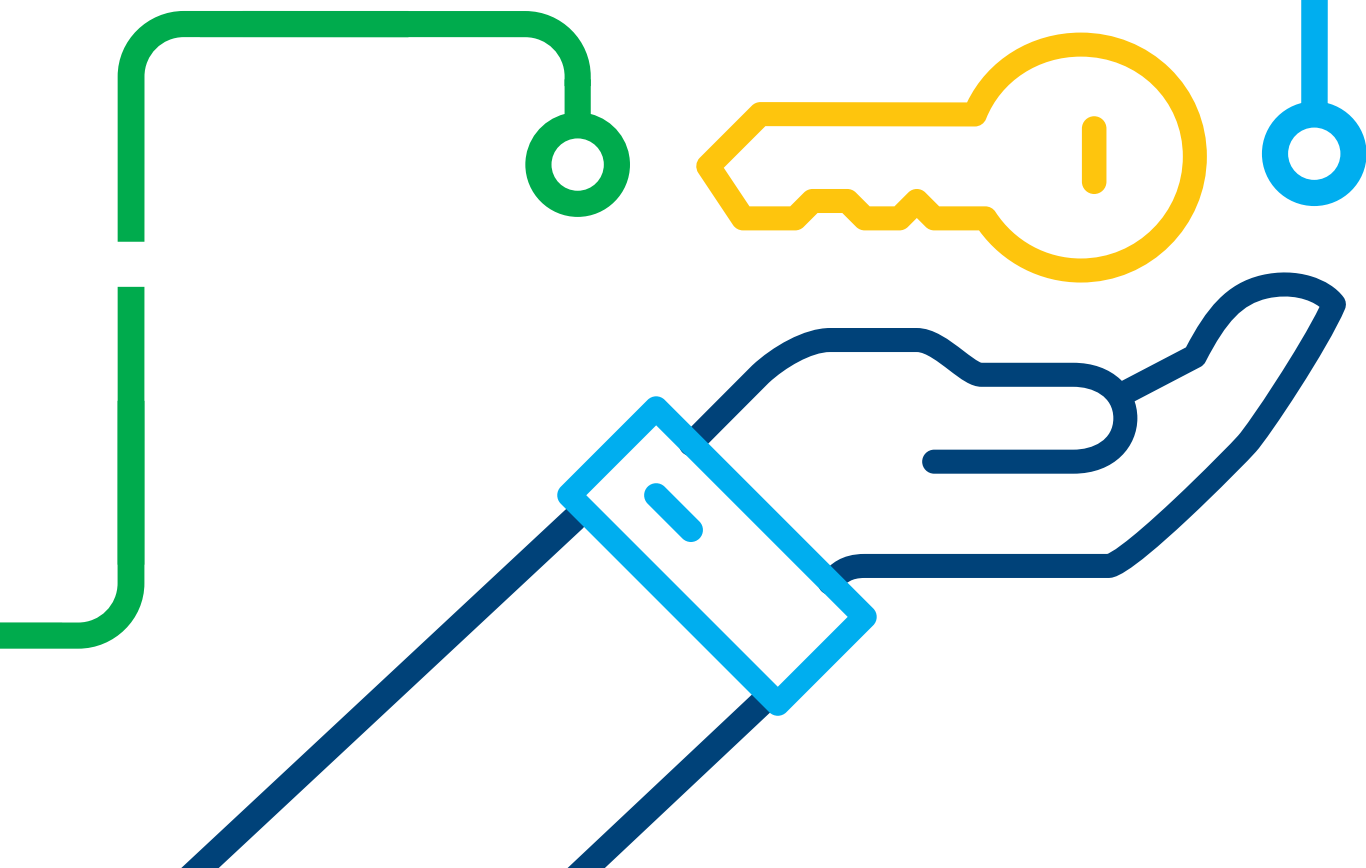
Back Up Your Princt Servers

After you have made all these changes, it is time to back up your work. Your time and efforts are valuable, and you need to ensure that effort is protected. Select whatever backup program you prefer, or the Windows Server Backup (built into Windows Server) – just ensure you back up the Systemstate and retain the backup off the Princt server itself – maybe even a duplicate off-site.

Maintaining a consistent backup is also an essential tool if a Ransomware attack succeeds. Having a solid backup will be critical to getting back up and running again as quick as possible saving you valuable time and money.

Document Your Work

Documentation is critical to your success. You should always document your work thoroughly and clearly; otherwise, it could make troubleshooting more difficult and time-consuming. Concise documentation will help with troubleshooting, audits, introducing new hardware and software into your plant, training of users, etc.



Train Your Employees

Just like with everything else, your employees must learn how to be responsible users. This takes education.

Security Awareness Training will cover:

- Understanding Information Security
- Ensuring data security
- Ensuring physical security
- “Best Practices” for safe computing including remote & mobile
- What to do if there is a threat or breach

Harden Your Infrastructure

Review your Network Switches and Firewall to look for the following:

- Replace “End-of-Life” products with newer, more secure products
- Update the firmware to the latest version
- Add a security banner if allowed
Security Banners are displayed upon login to both identify the switch as well as provide information about security and monitoring policies. In some jurisdictions, hackers who break into your system cannot be prosecuted unless you provide a banner that informs unauthorized users that their use is unauthorized. In other jurisdictions, you may be forbidden to monitor the activities of even unauthorized users unless you have taken steps to notify them of your intent. Legal notification requirements are complex and can vary by jurisdiction. Even within jurisdictions, legal opinions vary, and this issue should be discussed with your own legal counsel.

```
*****
* This system is restricted solely to <COMPANY NAME> authorized users *
* for legitimate business purposes only. The actual or attempted *
* unauthorized access, use or modification of this system is strictly *
* prohibited by <COMPANY NAME>. Unauthorized users are subject to *
* Company disciplinary proceedings and/or criminal and civil penalties *
* under state, federal, and * other applicable domestic and foreign *
* laws. The use of this system is monitored and recorded for *
* administrative and security reasons. Anyone accessing this system *
* expressly consents to such monitoring and is advised that if such *
* monitoring reveals possible evidence of criminal activity, <COMPANY *
* NAME> may provide the evidence of such activity to law enforcement *
* officials. *
*****
```

```
*****
* Location : Prepress Production / Wiring Closet A *
* Contact : Eugene F. O'Brien : (770) 794-6205 *
*****
```

- Disable unused features and enable security features based on vendor-recommended and industry-accepted “Best Practices.” Features you want to enable are things like Broadcast Storm Control, DHCP Snooping, IGMP Snooping, MLD Snooping, Dynamic ARP Inspection, and IP Source Guard. Features you want to disable are things like IP Fingering, Proxy ARPs, PAD Services, TCP and UDP Small Servers, UDLD, Web Servers, and Discovery Protocols.

Summary:

The items outlined in this white paper are suggestions based on years of frequently asked questions from printers. You may see various recommendations from other sources, but you must decide what makes the most sense for your plant. Each customer's security requirements are different. Heidelberg cannot make security decisions for our customers, nor can we enforce them.

As you define the security requirements for your plant, you should apply them to all the servers in your plant not just the Prinect servers; however, please keep in mind the requirements of any applications you will be running on other servers. Keeping all your servers hardened is a good strategy for helping to prevent breaches and protect yourself from the various threats. Hardening your Prinect servers is just one of the tools in your tool bag to remove any vulnerability that can be exploited.

Hardening your Prinect servers does not guarantee that you will never have a security incident. There are new threats emerging daily, and there are still users who fall prey to phishing attacks, etc. By hardening your Prinect servers, you are not eliminating the possibility of a successful attack but minimizing it. You need to make it as difficult as possible for someone to compromise your plant.



Please direct any questions regarding this document to
Eugene F. O'Brien, Senior Technical Support Analyst at:
(770) 794-6205 or
eugene.obrien@heidelberg.com

Heidelberg USA

1000 Gutenberg Drive

Kennesaw, GA 30144

Phone 800 437 7388

info@heidelberg.com

www.heidelberg.com/us

Trademarks

Heidelberg, Heidelberg logotype and Prinect are registered trademarks of Heidelberger Druckmaschinen AG in the U.S. and other countries. All other trademarks are property of their respective owners.

Subject to technical modifications and other changes.