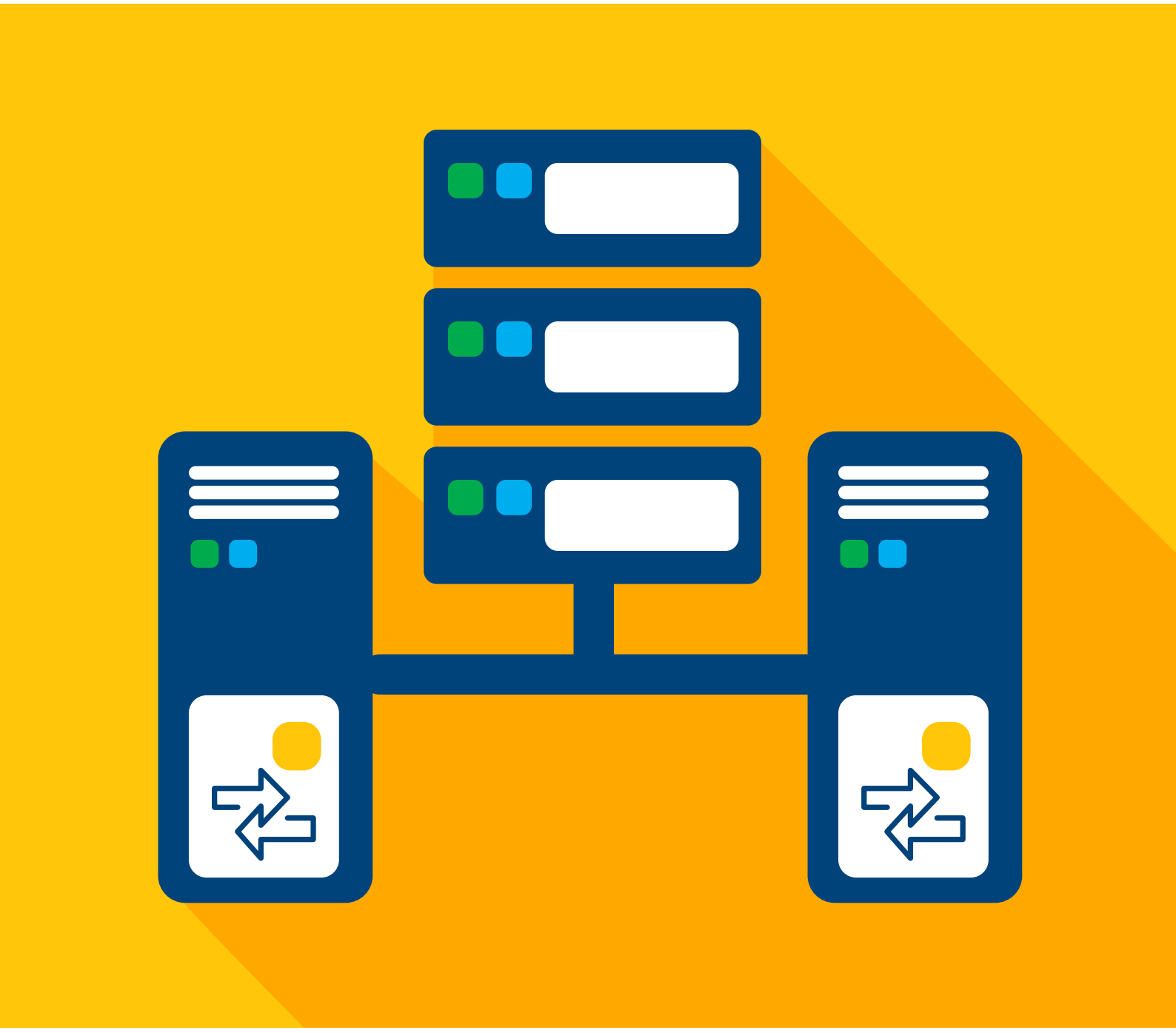
Prinect

Technical White Paper
Using Heidelberg Prinect Workflow in a Domain



HEIDELBERG

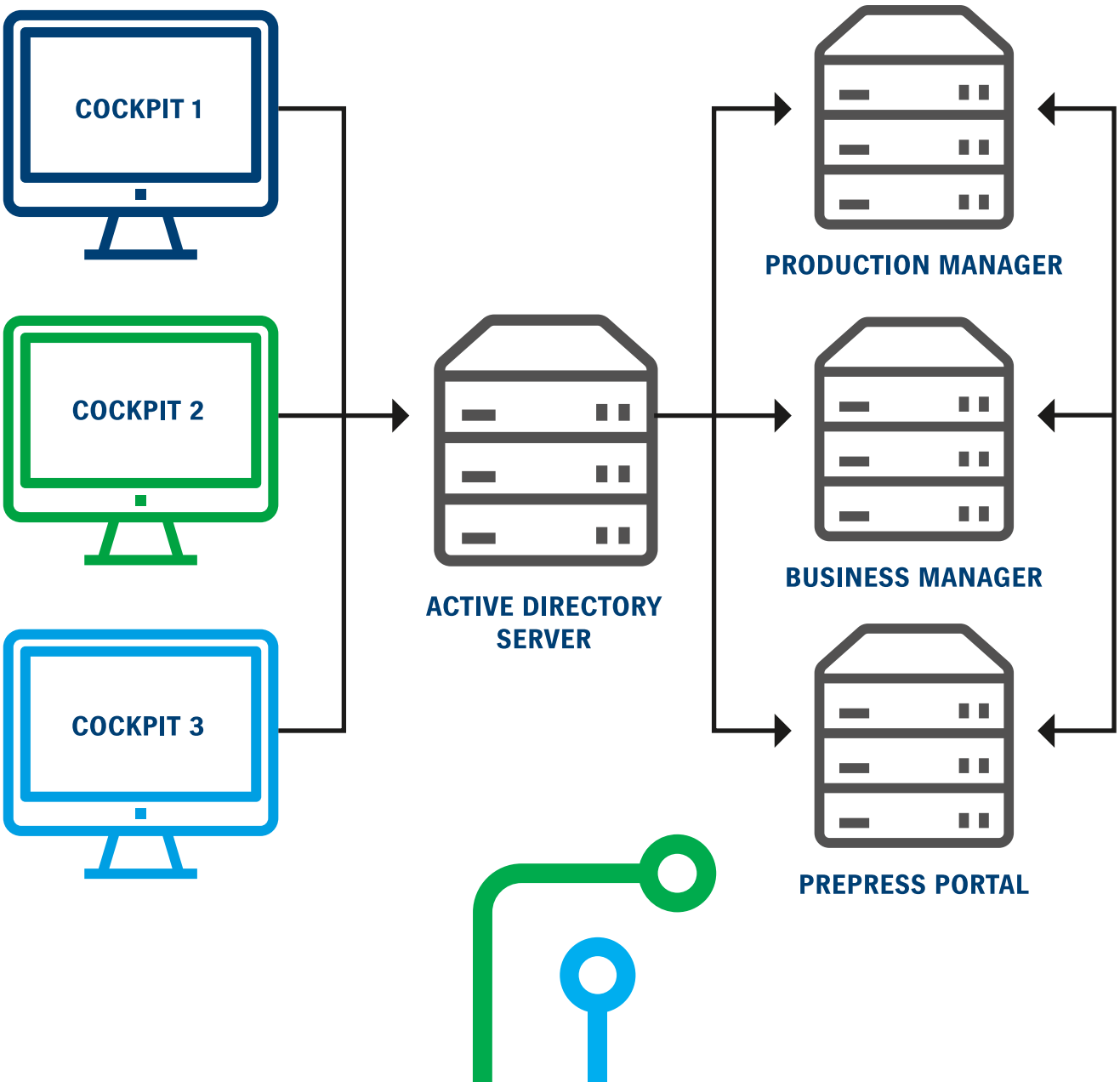
Heidelberg Prinect Workflow in a Domain.

Modern infrastructures, especially those that are larger or more complex, use directory services to organize and provide access to the network's devices and data. These directory services are more commonly referred to as "Domains."

If you do not feel comfortable implementing the Heidelberg Prinect® Workflow in a Domain, please consult with an IT Professional or Heidelberg Professional Services to assist you. Please note that you may not want to implement this during normal production hours as it could be disruptive.

Please Note: Implementing or troubleshooting a Domain is outside the scope of the normal product support capabilities of the Heidelberg Technical Help Desk.

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



Contents

*The information provided herein is being delivered to you "as is" and Heidelberg makes no warranty as to its accuracy or use. Any use of the technical documentation or information contained herein is at the risk of the user.

What is a domain?

A central security database:

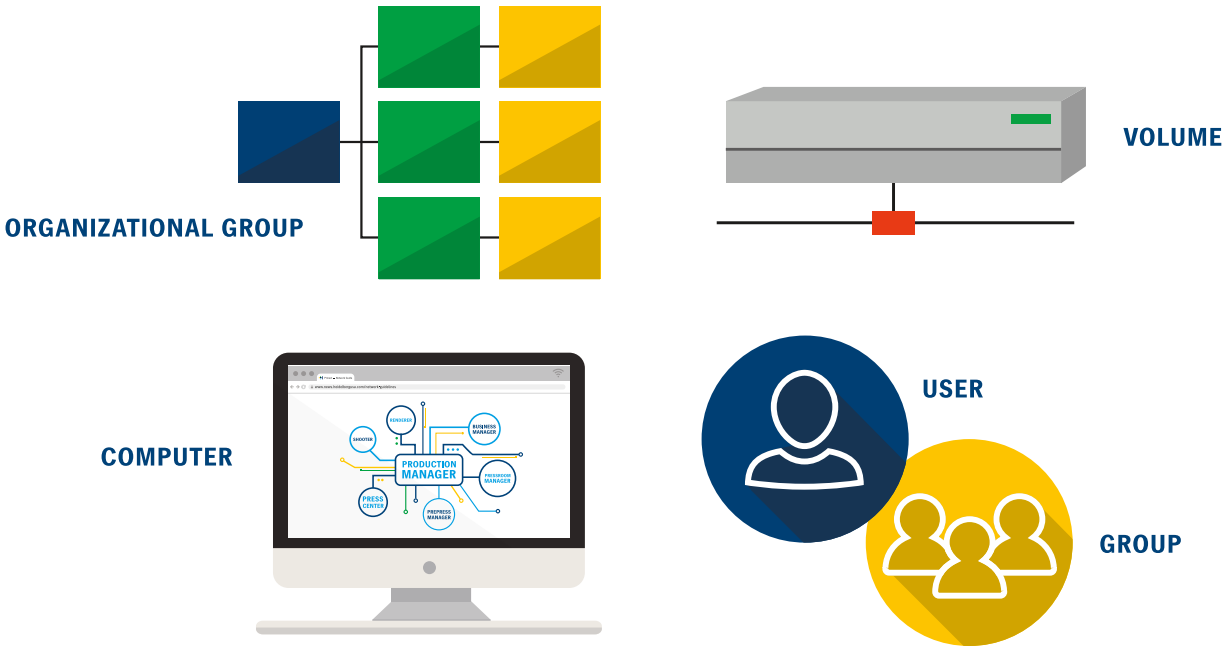
On a LAN (Local Area Network), a Domain is a central security database made up of a group of objects (users, groups, computers, printers, shared folders, etc.). Note that these types of Domains should not be confused with “Internet domains” like, for example, heidelberg.com; although there can often be a relationship between each type. Within a Domain, users authenticate once to a centralized server known as the Domain Controller (DC), rather than repeatedly authenticating to individual servers and services. Instead, the individual servers and services accept the user based on the approval of the Domain Controller.

Domains are based on a standard architecture that includes LDAP (Lightweight Directory Access Protocol) and Kerberos. LDAP is a protocol used over a TCP/IP network to talk to the Directory Services. Kerberos is a way for users and/or devices to prove their identity using “session tickets.” In fact, one way to view a Domain is with the security rights that each user is provided – these rights control access to various Domain objects.

Over the years, there have been several Domain architectures available such as Apple® Open Directory, Unix NIS (Network Information Services), Novell’s Network Directory Services (NDS), which eventually became Novell Directory Services and then eDirectory. When joining the Heidelberg Prinect Workflow to a Domain, we are referring to Microsoft® Active Directory (AD). Active Directory is often called a Windows Domain. Microsoft Corporation first introduced Active Directory in MS Windows™ 2000 as their entry into “Directory Services.”

Active Directory centralizes the administration of users/devices and allows for security policies to be applied on a more global basis so users become less tied to a specific workstation. As they login with their Domain credentials, they get access to their profile and data regardless of what workstation it is (as long as they have access to the various applications). For example, if you have to change passwords for a user, you would have to change them at every node in a Workgroup (and hope you do not make a typo) whereas with Active Directory, you just make the change once in one location. It is similar to how DNS eliminates the need for hosts files and DHCP eliminates the need for manual IP configuration at each individual node. Most customers that have an Active Directory Server also use it as their DNS Server, DHCP Server and NTP (Network Time Protocol) Server.

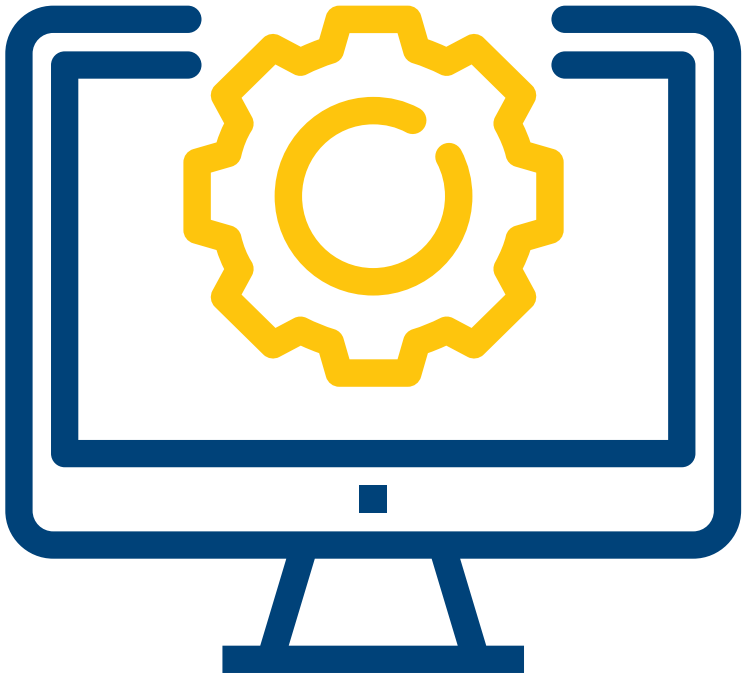
With people utilizing Terminal Servers to facilitate remote workers, Microsoft Terminal Server has required Active Directory since Microsoft Windows Server 2016.



What kind of hardware do I need for Active Directory?

For an Active Directory Server, you do not need a lot of CPU Cores or storage (although it definitely doesn't hurt) but you do want a lot of memory and good network I/O. While not mandatory, it is common that customers have a Primary and Secondary Active Directory Domain Server. The Secondary Active Directory Server becomes the failover in case something happens to the first Active Directory Server. You can, of course, add a Secondary later. If you decide to only have a primary Active Directory Server, you need to make sure you have built in redundancy like Hardware RAID, Redundant Power & Cooling, etc. as well as use a UPS with Battery Backup (preferably separate ones for each power supply connected to separate electrical circuits). I recommend a newer OS like Windows Server 2019 as the operating system as it is more at the start-of-life and easier than upgrading the OS on your Active Directory Server later.

You must make sure you have enough Client Access Licenses (CALs) to access the Active Directory Services at any time. You need 1 CAL (Client Access License) for each User (or device) using the Active Directory Services. You can increase CALs at any time, but you cannot decrease licenses once you add them. Most servers only have a few users, but Active Directory has all the users because it is a central database of all logins. Within Prinect, a production user logs into Cockpit or Business Manager or wherever (Data Terminal, Press Console, etc.) using their Domain account, which then gets authenticated with the Active Directory Server to determine their Privileges, Permissions and Rights.



Can I use the Heidelberg Prinect Workflow in a Domain?

Not only can you use the Prinect Workflow in a Domain, but Heidelberg strongly recommends it. The alternative is to install in a Workgroup; however, Workgroups only make sense in very small environments or homes. Workgroups can become more cumbersome and time-consuming to manage and maintain as you scale up and scale out your network. In addition, Workgroups are prone to simple mistakes such as typos or forgetting to modify one node that can wreak havoc in your Workflow.

Heidelberg recommends installing the Heidelberg Prinect Workflow directly into a Domain rather than join it to the Domain later. It is easier to set-up user accounts and devices without having to configure them on different machines; particularly, as changes are made in the future and propagated everywhere. When you are joined to the Domain, you don't have encounter all the issues that can arise with mismatched host tables, user access to shares, etc. because a Domain provides a central way to manage users, devices, services and various other objects as well as the trust relationships between them. Being on a Domain can also control access to services in the plant such as e-mail or Internet access.

You cannot, however, have some Workflow components joined to the Domain and some Workflow components not joined to the Domain. This would result in unexpected behavior in your Heidelberg Prinect Workflow that would be very difficult to rely on and troubleshoot. For example, a device in a Microsoft Active Directory Domain can access resources outside of the Domain (providing they have access rights to it) but the Non-Domain device would not be able to authenticate to the Domain and would need to be a member of the Domain to connect to the Domain's resources. Additionally, there are no automated updates or controls over policies and password aging, so if an account's password changes, it can break the workflow.

Guidelines for Joining the Heidelberg Prinect Workflow to a Domain:

Heidelberg has several recommendations when using the Heidelberg Prinect Workflow in a Domain.

- Do NOT make any Prinect Servers the Domain Controller.
- If running in a virtual environment, do not run any Prinect virtual machines on the same Virtual Host Server as a Domain Controller virtual machine (VM). While you can run on Active Directory on a VM, Microsoft recommends that you always have at least one Domain Controller that is on physical hardware so that failover and infrastructure can start. The time on the Virtual Host and the ADS VM must be in sync. In addition, the Virtual Host must be able to resolve the Primary and Secondary ADS DNS names. Since the ADS is typically the NTP Server and DNS server, and these may not be available yet when booting, you could experience some disruption caused by the confused environment. You may want to have a Physical Primary ADS server and a Secondary one in a VM.

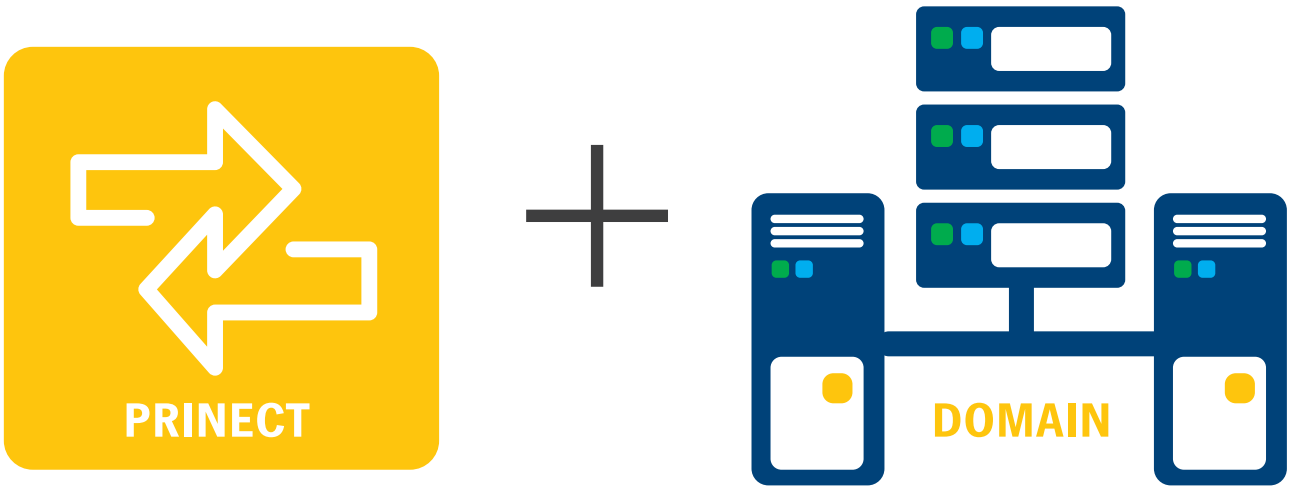
Also note that VMWare® provides a default ADS Group named “ESX Admins” that automatically gets added to each host. This group is granted full administrative rights by default, which could indirectly compromise security. You want to select the Domain users who get assigned to the “ESX Admins” Group. **Please Note:** This group is not automatically created in Active Directory. An administrator must manually create the group; once created, all users that are members of this group get full admin access to all vSphere hosts added to the domain.

- Network Time is critical in a Domain. When installed in a Domain, all Prinect Workflow components should be configured to synchronize their clock to the Domain Controller. The Domain Controller synchronizes to an atomic clock on the Internet.

- You have to consider the version of Active Directory being used. When someone asks if the Heidelberg Prinect Workflow will run on their Domain, the answer is yes; however, Heidelberg does not sell or install the Domain controller. We assume you will be using either 64-bit Microsoft Windows 2019 (preferably), Microsoft Windows Server 2016, or Microsoft Windows Server 2012 R2. If you are using an older version like MS Windows 2008 R2, MS Windows 2003 or MS Windows 2000 for your Active Directory, you could experience undesired results due to various problems such as mismatched encryption types. In addition, these Operating Systems have been made end-of-life by Microsoft and some are 32-bit. You should consider planning a migration in the near future to take advantage of increased memory, security, performance and functionality that the newer Operating Systems provide. We also assume that Active Directory was setup by someone knowledgeable with configuring Domains and that follows vendor-recommended and industry-accepted “Best Practices.” Finally, the Domain Controller is a core component of your infrastructure so we assume this is running on hardware that performs well and has some availability.

- Similar to the version of your Domain Controller, the version of Prinect matters. Newer versions of Prinect are more suited to Domain environments because they support the newer server and client Operating Systems, and there have been many improvements over the years to those environments that improve how reliably they perform. So, when you ask can the Heidelberg Prinect Workflow work in your Domain, we assume you are using one of our latest versions like Prinect Version 2020.10 and not Version 2009.

- Often a customer’s workflow includes third party components that can be outdated. We do not know the implications of joining third party or old systems to your Domain.



Guidelines Continued:

- Avoid using Prinect in a .local Windows domain or top-level DNS domain (sometimes called the first-level Domain name). This would include cases where you use a sub-domain like xyz.local, for example. Note that this is not really a Prinect issue but more of an issue related to Apple Mac OS X, and most customers have some Mac clients running Prinect Client applications like Cockpit.

  Unfortunately, it is quite common to find .local Windows Domains; most likely, this was used in the Active Directory documentation or training or is the default in some setup scripts. The "Best Practice" way to name an Active Directory domain is to create a subdomain that is the delegation of a parent domain that you have registered and can control. For example, if I use my Internet-facing website heidelberg.com as my company's site, I should name my Active Directory domain internal.heidelberg.com or something similar. You also want to avoid the issues associated with using heidelberg.com for the both the Internet-facing zone and the internal zone.

  Using a .local Windows Domain can result in issues – particularly with Apple Macintosh OS X implementations. They rely on Multicast DNS (mDNS) to allow computers on a small network without a DNS Server to provide IP networking with the auto-configuration and ease-of-use for which AppleTalk was known. Basically, each computer knows its own name and responds to requests for that name automatically via IP multicast.

  One problem is that across different versions of the Mac OS X, Apple has changed how it works. For example, with the Macintosh OS X version 10.10 (Yosemite), Apple enforced reserving the .local TLD (Top Level Domain) for Bonjour. Unfortunately, this is different from how things worked in previous versions. These changes can create problems as people make assumptions on how things work based on past behavior or certain settings that are hard coded. To get the same behavior with Apple Mac OS X version 10.9 (Mavericks) in the Version 10, you have to enter the following command in a Terminal window:

  ```
  sudo discoveryutil mdnsactivedirectory yes
  ```

  All of this can be avoided by not using a .local Domain. The .local domain name is not registered on the Internet. Hostnames ending with .local in private networks must be resolved by a local DNS server. There can be a problem resolving these .local names via typical unicast DNS servers because of a move towards zero-configuration networking. For more information, please consult Apple (see **https://support.apple.com/en-us/HT203136**). If you want to change the name of your Active Directory Domain, Microsoft has documents and tools that allow you should consult to do this, see **https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc786120(v=ws.10)**). As always, if you do not feel confident and comfortable in doing this yourself, consider bringing in an experienced professional.

  Some people are unable to change their Domain name. We do have some customers running on a .local Domain that have reported no issues. If your Windows Domain uses .local, you need to put the word "local" in the "Search Domains" field in the DNS settings in the network panel. You also need to use your Active Directory Domain Controller as your DNS server, and ensure you have setup the Start Of Authority for the Domain name in your local DNS Server.

- A couple of Domain Policies that we have seen cause issues depending how your Domain is configured:

  Log on as a Batch Job: This policy can impact/prevent the ability to run the DB Maintenance (Prinect_BU) Scheduled Task. In many cases, IT Departments do not mind granting this permission to the Prinect Services user, but in a couple of cases we have had customers that have only one special user in the AD\Domain that is granted this permission. So this user is set in the Configurator to run the backup and of course added to the MS-SQL users.

  Allow Log on Locally: In one case, remote Cockpits could no longer connect to the Prinect server due to this policy not being granted. In testing this setting, it seems that this permission was not explicitly required prior to Prinect 2020.

- Of course, you must harden the domain servers (see **https://bit.ly/security-best-practices**).

As always, I strongly recommend that you have a Prinect Software Maintenance Agreement for your Heidelberg Prinect Workflow.

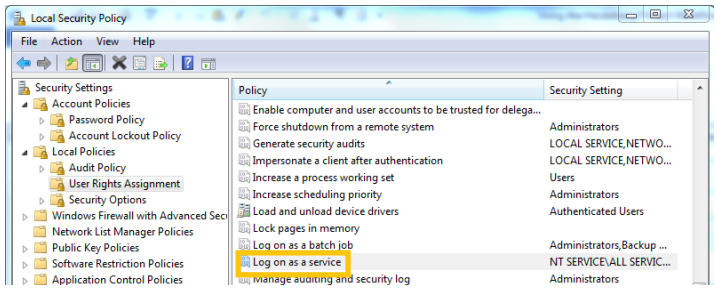
How do I join a Heidelberg Prinect Workflow to MY Domain?

Prinect Servers

There is nothing unique for joining Prinect to your Domain other than the Prinect Installer requires that you have "Enable NetBIOS over TCP/IP" checked in the WINS Properties of the Advanced TCP/IP Settings for WINS. You join your Prinect application servers (Prinect Prepress Manager, Prinect Portal, etc.) the same as joining any MS Windows Server to a Domain; i.e., it is not Prinect-specific. However, once your Prinect server is joined to your Domain, you need to create a main Domain user account for the Prinect administrator user (usually "prinect"). This account must have Local Administrator Rights on the Prinect server but does not need Domain Administrator Rights. Once created, you need to switch the Prinect services to use the Domain Prinect user account because, by default, the Prinect services are started by the Local Prinect user.

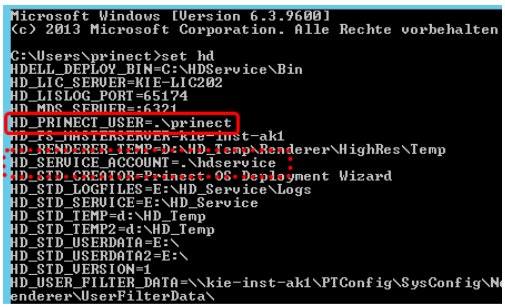
Use Windows Computer Management/Services to manually change the old\local prinect user designated for Prinect Supervisor service start to your new AD\Domain prinect user. Additionally, if you have other servers running the Prinect Supervisor service (for example, Renderer or Prepress Portal), you must make the same change needed to be done on those servers as well This requires that you set the "Log on as a service" in the User Rights Assignment of the Local Polices. **Please Note:** If these are pushed down from the Domain Controller, then you have to take care of it at that level.

1



Then follow the procedure in the next section on *"How do I configure Microsoft SQL Server used in Prinect for the Domain?"*

2



Keep in mind that there is a difference between joining Prinect to your Domain as part of a fresh installation and joining an existing Prinect installation to your Domain. This is because when you do it at initial installation, there are no user accounts to deal with. In addition, the Prinect environment will be wrong if joined to your domain afterwards:

The environment installer has to be started (in "expert mode") afterwards to correct the settings.

When the server is joined to a Domain, the Prinect Cockpit users can be configured to use their Domain credentials when they log in to Cockpit. Selecting "Password for OS Login" disables the password fields and enables the Domain field. If the option "Password for OS Login" is selected, the Prinect MDS (Master Data Service) uses a DLL from Supervisor that requests the user permissions from the Windows Operating System. At this point, you enter the Domain, and you do not define a password. When someone logs into the Prinect Cockpit, he will use his Domain password, and Prinect will authenticate the user via the Domain.

3

Prinect Servers Continued

The Prinect Cockpit works in a Workgroup the same way as in a Domain. On a Domain, you should create a group “Prinect Operators” inside the Domain (<Domain>\Prinect Operators) and add this group to the local group “Prinect Operators” on the Prinect servers to take advantage of the security.

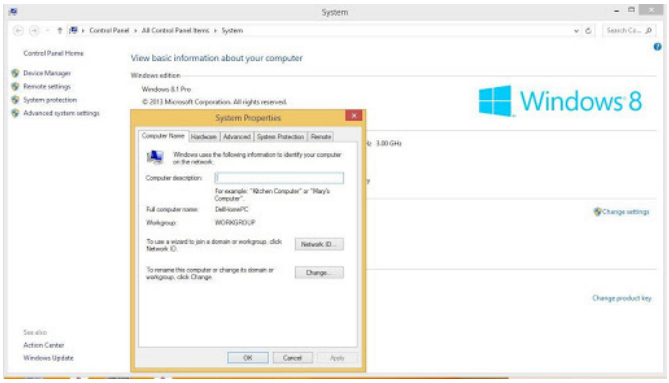
Please Note: You can run into trouble if you choose the default password age policies. Changing the Prinect Service User password is not supported (even when updating all Prinect services passwords manually in the services administration console). By selecting the default setting, you switch off any Remote Update/Upgrade possibility because the Prinect installer saves encrypted Prinect Service account/password information in the user registry that has been chosen at installation time, and those credentials will be used during update. Any following Remote upgrade will fail; you will have to perform a manual update to ensure that the stored information gets updated.

You can also encounter issues if you choose the default password complexity policies. Any Suprasetter container software update will fail (this password is not user defined), and any update that tries to configure the “prinect” or “hdservice” user will fail as well.

Prinect Clients

Any desktop workstations that will run Prinect Clients, e.g., Prinect Cockpit or Prinect Signa Station, should be joined to the Domain. Then you can log in with your Domain User Account.

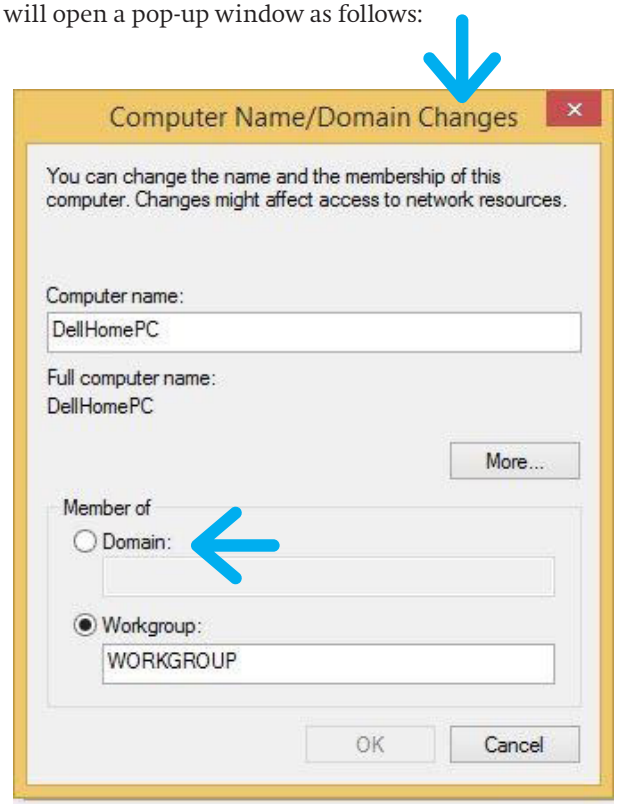
1



On a MS Windows workstation, go into the “Advanced system settings” for the computer and under the “Computer Name” tab click the “Change” button. Note there may be subtle differences across different versions of your Operating System.

This will open a pop-up window as follows:

2



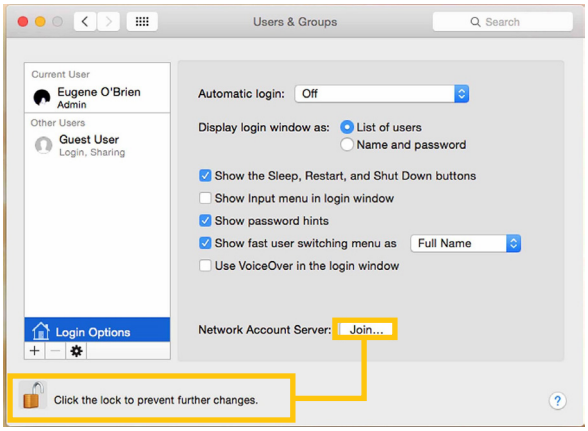
Change the radio button to “Domain:” under the “Member of” area and then type the name of your Domain – get this from your System Administrator.

Now you should be able to log off the current local user you are logged in as, then login to the PC with your Windows Domain credentials. Then use your Domain user account to login to the Prinect applications.

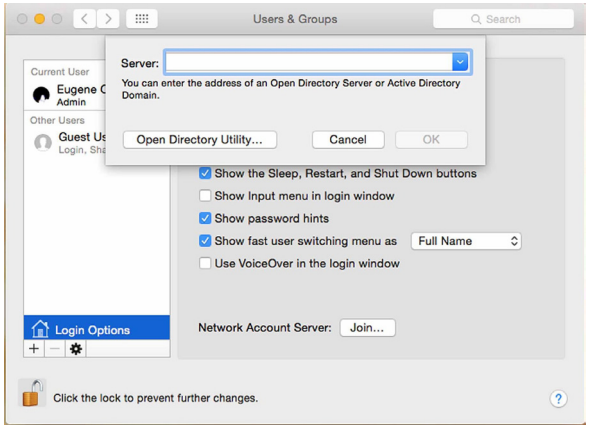
If you are using an Apple Macintosh computer, then open the System Preferences and click on the Users & Groups. Next click the Padlock to make changes to these settings. **Please Note:** This will open a pop-up window asking for your user account and password. Make sure you use your local Admin account on the Mac and not a Windows account or Domain Account.

Next, click the "Join" button next to "Network Account Server." Enter the IP Address of your Windows Active Directory server and click the "OK" button. It should find the Active Directory server. If it doesn't find it, you will get the spinning wheel. If it does find it, it should populate the next window with the server hostname and ask for the Active Directory Domain Admin account and password.

1



2



Proofer Devices and Digital Printers

In an "integrated workflow", you may have several third party products implemented. For example, the integration of most Canon® production printers is done via JDF/JMF to their EFI-based Fiery Print Controllers or an Oce/Canon Prisma Sync Print controller. Those print controllers are Microsoft Windows-based and can be configured for either a Workgroup or a Windows Domain. So, in principle, you would join the Domain, synchronize the clock to the AD Server, and login with a Domain user account. I recommend you consult your vendor for the most up-to-date information.

Press and Postpress

In these cases, you should consult the installing technician to make sure things are connected as you need.

Print Shop Infrastructure Appliances

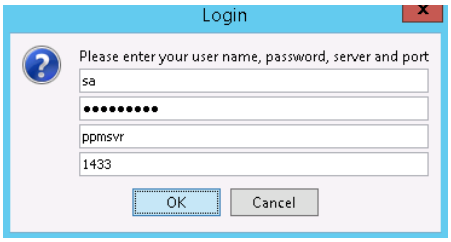
Certain components like Firewall Switches, Storage, etc. can become part of Active Directory domain and provide either authentication or, where applicable, file services to the domain users and applications.

In order to join these types of devices to your Domain, you will need access to a Domain Administrator account to add them to your Domain. The specific details, however, are outside the scope of this document and you should refer to the documentation, training and support of those vendors.

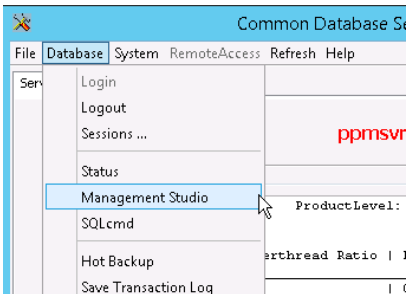
How do I configure Microsoft SQL Server used in Prinect for the Domain?

Once the Prinect services run under a Domain account, then you have to add that Domain account as a new login to Microsoft SQL Server and assign it to the sysadmins group in the MS SQL Server. This is so that the Prinect Backup will successfully run. The instructions below outline how to add a user (domain user or other user) to the MSSQL login and give that user admin credentials. This should be the account that the Prinect services are using.

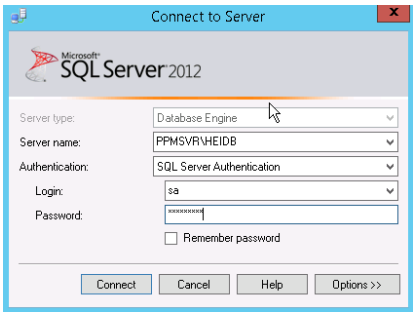
1 Log in to the Heidelberg DBService tool.



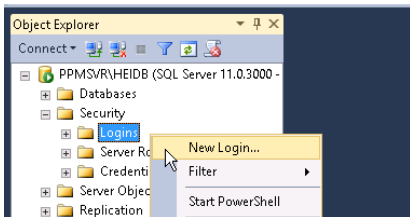
2 Go to Database > Management Studio



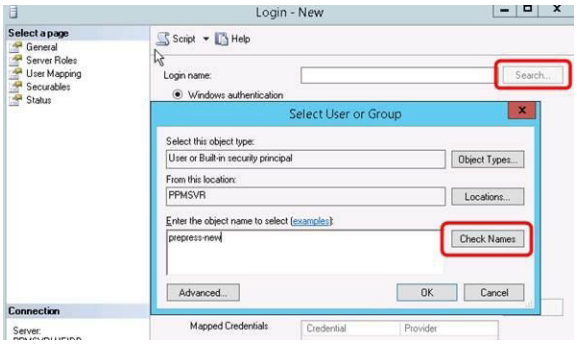
3 Connect to Server using SQL Server Authentication, NOT Windows Authentication. Use the sa User with the correct password for that account. (Of course, we don't like to publish passwords in documentation).



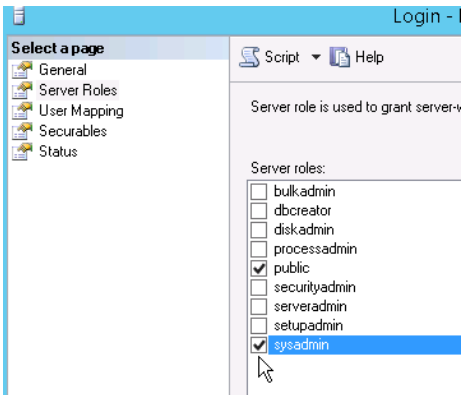
4 Go to Server name > Security > Logins. Right click and select New Login.



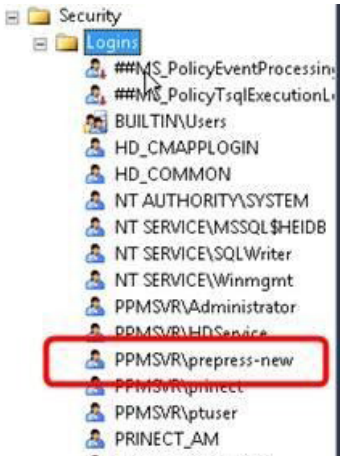
5 Click Search then enter the username that the services are running under. Click Check Names then OK.



6 Select Server Roles under Select a page. Check sysadmin then OK.



7 The user will now appear in the Logins list.



Final Steps.
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 as well as make future scaling out or up of your environment more difficult. Concise documentation will help with troubleshooting, audits, introducing new devices or users into your plant, etc.

The main issues we encounter using the Heidelberg Prinect Workflow in a Domain are usually related to someone implementing security policies. They change some things and then other things don't work, and they don't have a change log of what they did. So, it is very important to document your environment thoroughly.

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. Heidelberg cannot make infrastructure decisions for our customers, nor can we enforce them.

Note that Microsoft has been driving customers towards Azure Active Directory their Cloud-based solution. At this time, Heidelberg cannot provide guidance on that solutions. If considering it, please perform your due diligence in understanding costs, technical limitations, performance, etc.

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