Privileged Access Workstation (PAW)

Viktor Hedberg, Mikael Nyström, Hasain Alshakarti

Truesec AB
Oxtorgsgränd 2, 111 57 Stockholm
info@truesec.se
www.truesec.com

TRUESEC

Table of Contents

Truesec AB
Corp ID: 556676-3073
www.truesec.com

Sweden
+46 810 00 10
info@truesec.se

US
+1 (425) 818-8044
info@truesec.com

Summary

This document aims to describe the concept of Privileged Access Workstations (PAWs) and the implementation of the same. The document will cover the why's, when's, and how's of PAWs, as well as giving examples of how many PAWs an administrator will need when performing administrative activities towards an IT environment. It will also cover examples on how to configure PAW setup within any organization. The setup may vary dependent on laws and regulations governing privileged access within the organization.

Truesec AB
Corp ID: 556676-3073
www.truesec.com

Sweden
+46 810 00 10
info@truesec.se

US
+1 (425) 818-8044
info@truesec.com

1. Privileged Access Workstation

1.1. Why should you use it?

A privileged access workstation (PAW) protects the administrators' credentials from being abused using various techniques. Implementing PAWs further solidifies the Tiering concept in an Active Directory environment as the admin accounts only can perform administrative activities from a dedicated workstation.

Here are some of the techniques and methods commonly used to steal and tamper with administrator credentials made significantly harder by using PAWs:

- Pass the hash
- Pass the ticket
- Password dumping
- Lateral movement

The PAW should be configured in such a way that it is minimalistic when it comes to 3rd party applications, and hardened by using Windows built-in security features, such as credential guard, app guard, and exploit guard. Outbound traffic from this device should be restricted to a very limited set of permitted destinations.

By keeping the admin accounts and PAWs under strict control, we can effectively limit a potential threat actor's ability to compromise the environment.

Truesec AB
Corp ID: 556676-3073
www.truesec.com

Sweden
+46 810 00 10
info@truesec.se

US
+1 (425) 818-8044
info@truesec.com

1.2. What is tiering and how does it relate to PAWs?

Tiering is a way to define security layers using controls and restrictions within any type of IT environment, they are usually defined as follows:

1.2.1. Tier -1 (Backup)

Also known as the backup plane, if you have access to this you can control the backup infrastructure of the IT environment in general. This Tier should be isolated from the production environment and the fabric plane. The reason for this is that a T0 account, if compromised should not have access to the virtualization platform. This can be achieved by placing the Tier -1 in its own Active Directory Domain.

1.2.2. Tier -1 (Fabric)

Also known as the fabric plane, if you have access to this you can control the virtualization platform and the backbone of the IT environment in general. This Tier should be isolated from the production environment. The reason for this is that a T0 account, if compromised should not have access to the virtualization platform. This can be achieved by placing the Tier -1 in its own Active Directory Domain.

1.2.3. Tier 0

Also known as the control plane, if you have access to this you can control everything and do anything. Domain Controllers, Azure AD Connect Servers, Certificate Authority servers and equivalent systems on-premises as well as being Global Admin in Azure.

1.2.4. Tier 1

Also known as operational plane, here are basically all member servers in a domain, or standalone servers in azure, including services or resource groups in Azure. Having access to Tier 1 systems means you can partially compromise the organization

1.2.5. Tier 2 or Tier E

Also known as client control, here is where you have access to all or some client devices

More information on tiering can be found in a separate document describing the concept of tiering in detail.

Truesec AB
Corp ID: 556676-3073
www.truesec.com

Sweden
+46 810 00 10
info@truesec.se

US
+1 (425) 818-8044
info@truesec.com

1.3. When should you use it?

A PAW should be used when performing any administrative activity towards Tier -1, Tier 0, Tier 1, and in some cases even Tier 2 or Tier E require the use of a PAW. Therefore, the use of PAWs is not a technical decision, but in fact a business decision.

1.4. How should you deploy and configure your PAWs?

The fundamental regarding deployment of PAW is the chain of trust, each part must be trusted. Example, if someone else can borrow your PAW, it is no longer considered to be safe to use.

The basic idea is that you need one PAW for each account and environment you are accessing, for example. If you have one Active Directory Domain, and two different administrative account, you need two PAWs. This could result in having many PAWs, and each of the could be a laptop, carrying 45 laptops is not practical, therefore, in most situation you could use a physical computer as you PAW Host running Hyper-V and on top of that, run multiple virtual PAWs, below is a list of different configurations.

1.4.1. The personal device

You always need a personal device (also known as a companion device), this could be any type of computer, laptop, desktop, tablet or even a phone. You will never perform any administrative work on device. This could be a physical computer, or it could be a virtual machine. (Details will be covered in the configuration examples)

Truesec AB
Corp ID: 556676-3073
www.truesec.com

Sweden
+46 810 00 10
info@truesec.se

US
+1 (425) 818-8044
info@truesec.com

1.4.2. PAW Configuration example 1

Scenario: You are assigned a T0 account for on-premises Active Directory

Your configuration:

Option 1:

You have one companion device and one physical PAW. The PAW is joined to the same domain being managed. For this to be ok, tiering must be implemented.

Option 2:

You have one physical laptop, acting as PAWHost. On the physical computer, you have two virtual machines, one virtual companion device and one virtual PAW. The PAWHost is joined to the same domain being managed.

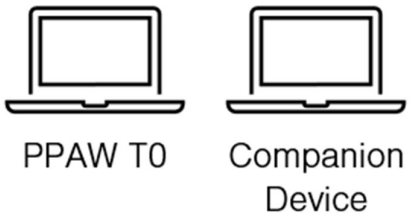

Figure 1 Physical PAW T0 and physical Companion device

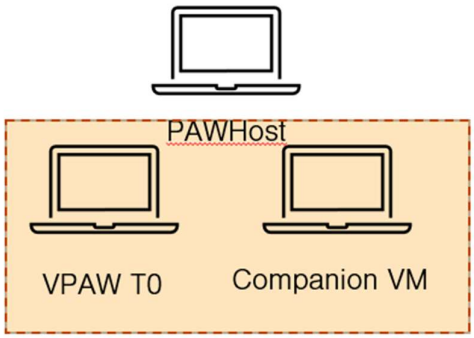

Figure 2 PAWHost with Virtual PAW TO and Virtual Companion device

Truesec AB
Corp ID: 556676-3073
www.truesec.com

Sweden
+46 810 00 10
info@truesec.se

US
+1 (425) 818-8044
info@truesec.com

1.4.3. PAW Configuration example 2

Scenario: You are assigned a T1 account for on-premises Active Directory

Your configuration

Option 1:

You have one companion device and one physical PAW. The PAW is joined to the same domain being managed. For this to be ok, tiering must be implemented.

Option 2:

You have one physical laptop, acting as PAWHost. On the physical computer, you have two virtual machines, one virtual companion device and one virtual PAW. The PAWHost is joined to the same domain being managed.

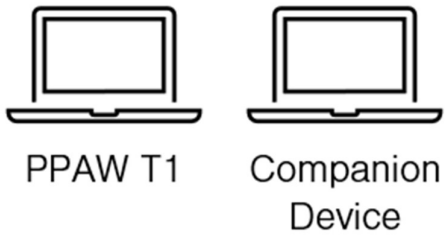

Figure 3 Physical PAW T1 and physical Companion device

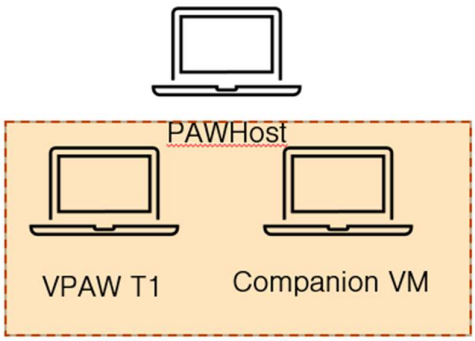

Figure 4 PAWHost with Virtual PAW T1 and Virtual Companion device

Truesec AB
Corp ID: 556676-3073
www.truesec.com

Sweden
+46 810 00 10
info@truesec.se

US
+1 (425) 818-8044
info@truesec.com

1.4.4. PAW Configuration example 3

Scenario: You are assigned a T0 account for on-premises Active Directory and a T0 account for Azure Active Directory

Your configuration

Option 1:

You have one companion device and two physical PAWs. The on-premises PAW is joined to the same domain being managed. The cloud PAW is joined to the Azure AD tenant being managed. For this to be ok, tiering must be implemented.

Option 2:

You have one physical workstation, acting as a PAWHost. On the physical computer you have separate virtual machines for each workload. One for T0 on-premises, joined to the same domain being managed, one for T0 in Azure Active Directory, joined to the Azure AD tenant being managed, and one virtual companion device. The PAWHost is joined to the same domain being managed.

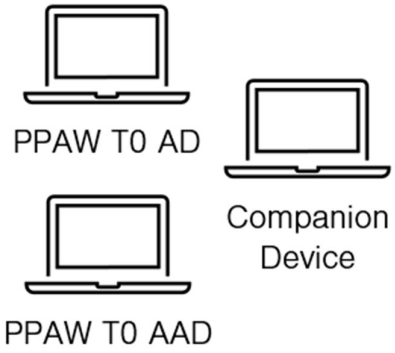

Figure 5 Two physical PAWs T0 and one physical Companion device

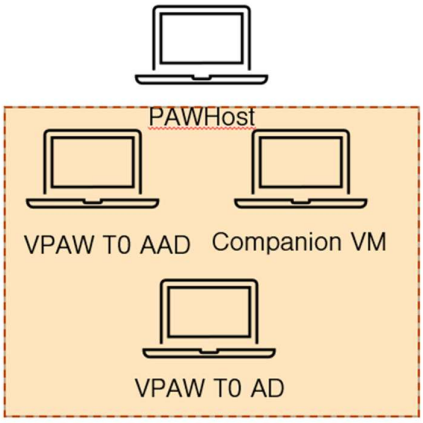

Figure 6 PAWHost with two virtual PAWs T0 and one virtual Companion device

Truesec AB
Corp ID: 556676-3073
www.truesec.com
Sweden
+46 810 00 10
info@truesec.se
US
+1 (425) 818-8044
info@truesec.com

1.4.5. PAW Configuration example 4

Scenario: You are assigned a T1 account for on-premises Active Directory and a T1 account for Azure Active Directory

Your configuration

Option 1:

You have one companion device and two physical PAWs. The on-premises PAW is joined to the same domain being managed. The cloud PAW is joined to the Azure AD tenant being managed. For this to be ok, tiering must be implemented.

Option 2:

You have one physical workstation, acting as a PAWHost. On the physical computer you have separate virtual machines for each workload. One for T1 on-premises, joined to the same domain being managed, one for T1 in Azure Active Directory, joined to the Azure AD tenant being managed, and one virtual companion device. The PAWHost is joined to the same domain being managed.

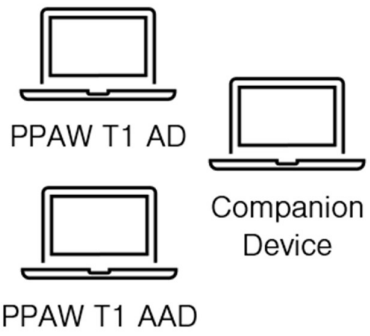

Figure 7 Two physical PAWs T1 and one physical Companion device

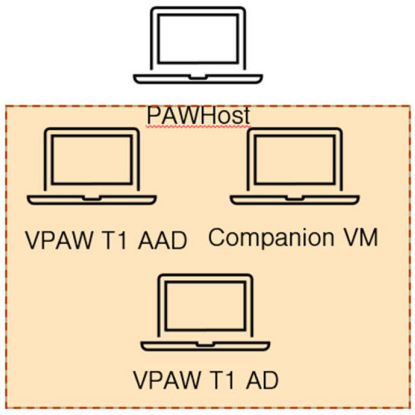

Figure 8 PAWHost with two virtual PAW T1 and one virtual Companion device

1.4.6. PAW Configuration example 5

Scenario: You are assigned a T-1 account for the fabric and a T0 account for the on-premises Active Directory

Your configuration

Option 1:

You have one companion device and two physical PAWs. The PAWs are joined to the same domain being managed. For this to be ok, tiering must be implemented in both domains.

Option 2:

You have one physical laptop, acting as PAWHost. On the physical computer, you have three virtual machines, one virtual companion device and two virtual PAWs.

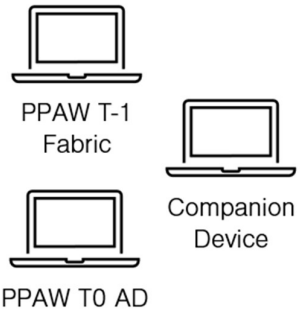

Figure 9 One physical PAW T-1 Fabric, one physical PAW T0 AD and one physical Companion device

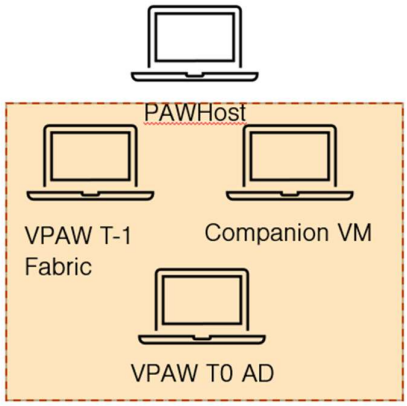

Figure 10 PAWHost with one virtual PAW T-1 Fabric, one virtual PAW T0, and one virtual companion device

1.4.7. PAW Configuration example 6

Scenario: You are assigned a T-1 account for the fabric, a T-1 account for the backup, and a T0 account for the on-premises Active Directory

Your configuration

Option 1:

You have one companion device and three physical PAWs. The PAWs are joined to the same domain being managed. For this to be ok, tiering must be implemented in all domains.

Option 2:

You have one physical laptop, acting as PAWHost. On the physical computer, you have four virtual machines, one virtual companion device and three virtual PAWs.

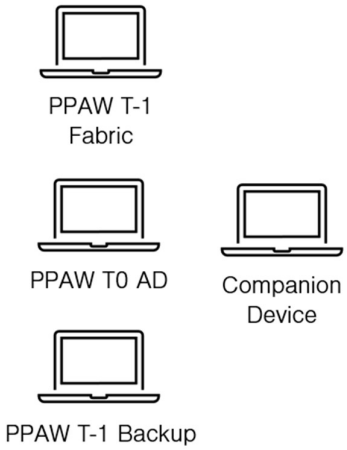

Figure 11 One physical PAW T-1 Fabric, one physical PAW T0, one physical PAW T-1 Backup, and one physical Companion device

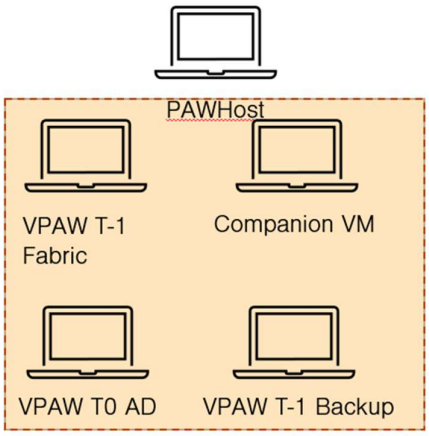

Figure 12 PAWHost with one virtual PAW T-1 Fabric, one virtual PAW T0, one virtual PAW T-1 Backup, and one virtual Companion device