



EPAS Proof of Concept (PoC) Implementation Process for Microsoft Active Directory[®]

Introduction

The current document describes the operational, network and physical requirements in order to perform an EPAS proof of concept installation at the customer's premises. It also gives a short overview over the encryption implementation which safeguards the customer's data. The description of EPAS and the results of the audit are mentioned in different documents and / or presented directly to the customer, based on the installation requirements.

EPAS is a hardware solution which is deployed in the customer's datacenter. The basic installation features two hardware components, the EPAS MASTER and the EPAS WORKER, which are to be installed in a datacenter rack.

After the proof of concept / installation, the customer can utilize EPAS in order to perform password audit reports, password analytics for multiple enterprise systems, ensuring privacy requirements are also met in this process.

Additional information on the enterprise systems that EPAS supports, and in-depth description of the functionality are found in separate documents, referenced here.

The document is structured in the following components / chapters:

Introduction	2
Installation & Training Overview	3
Physical/Datacenter requirements	4
Network and system requirements	7
Data Encryption – Trusted Computing.....	10

Installation & Training Overview

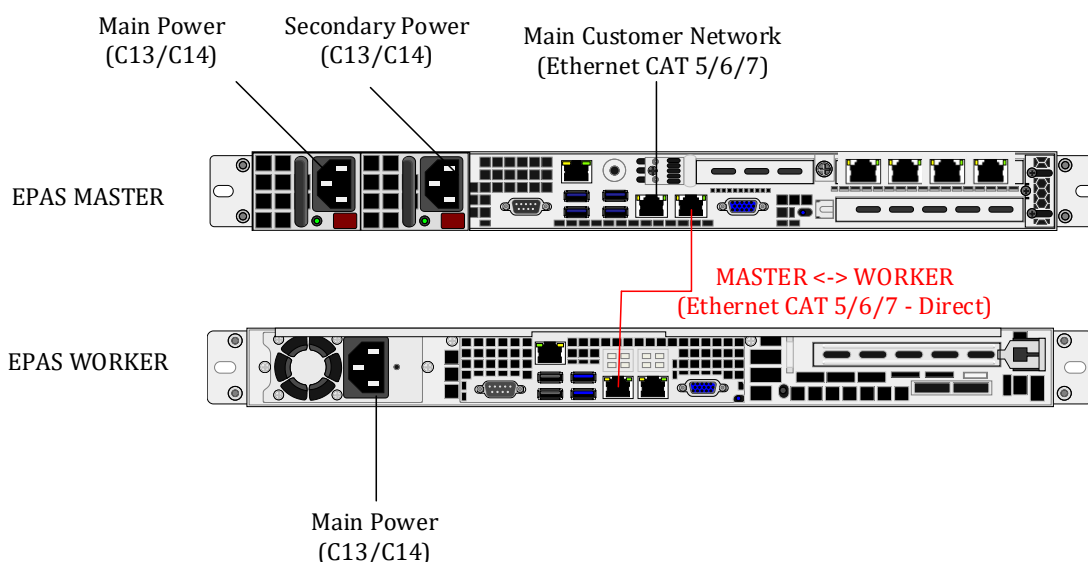
The EPAS proof of concept is performed at the customers premises. The PoC also includes installation and training, assisted by Praetors AG consultants. The goals of the installation and training period are:

- Physical installation of the EPAS appliances in the customer's datacenter
- Training for customer personnel in order to further utilize the product during the proof of concept
- Configuring two target systems in the EPAS management console, to be audited during the training period
- Providing short term overview of the password security in the above two target systems and presenting the results to the customer

Physical/Datacenter requirements

The current section addresses the physical requirements for the EPAS proof of concept, specifically related to installation of the physical component and other pre-requisites for the datacenter installation.

The following diagram shows a top-level overview of the cabling and racking of the units:





The following table details hardware components are shipped by Praetors AG and provided for the course of the PoC:

Component	Quantity	Notes
EPAS MASTER	1	Standard 19" 1U
EPAS WORKER	1	Standard 19" 1U
Rack installation kit (MASTER)	1	(Includes rail mounts and mounting bolts)
Rack installation kit (WORKER)	1	(Includes rail mounts and mounting bolts)

For the installation of the EPAS hardware components, the following table provides a list of requirements:

Requirement	Quantity	Notes
Rack space (MASTER)	1	Type: Standard 19" rack 1U Appliance dimensions (mm): 437x43x503

Requirement	Quantity	Notes
Rack space (WORKER)	1	Type: Standard 19" rack 1U Appliance dimensions (mm): 437x43x716
Power cables (redundant power inlets, if available)	2	Scope: EPAS MASTER Connector type: C13/C14 Power specification: 2x 100-240V/6-3A Connector layout: 
Power cable	1	Scope: EPAS WORKER Connector type: C13/C14 Power specification: 100-140V/14.7-10.5A 180-240V/10.5-8.0A Connector layout: 
Ethernet cable	1	Scope: EPAS MASTER to customer network Type: RJ45 Ethernet CAT 5/6/7 The network port should be enabled and ready for use when the consultant(s) are doing the on-site installation.
Ethernet cable	1	Scope: EPAS MASTER to EPAS WORKER Type: RJ45 Ethernet CAT 5/6/7 The connection is direct, only between the EPAS MASTER and EPAS WORKER. There is no requirement to connect this cable to any customer network equipment.

Requirement	Quantity	Notes
Datacenter access	N/A	Scope: During installation of the appliances Consultant(s) access to the datacenter for assisting in the hardware installation is recommended.

Additional information on the power requirements, dimensions and hardware requirements is found at the documentation endpoint (<https://www.epas.de/docs/audit/hardware/2-specs/>).

Network and system requirements

Given that the EPAS MASTER system is connected to the customer's network, the current section describes the network level requirements of EPAS, as well as the required connectivity and access rules to other systems.

Additional details on the requirements for each system type, as well as other features are available in the documentation endpoint (<https://www.epas.de/docs/>).

EPAS MASTER requirements

The EPAS MASTER system is connected to the customer's network. The following table lists the requirements for accessing the EPAS management console:

Requirement	Notes
Network allocation	Scope: EPAS MASTER An IP address, netmask and default gateway should be allocated to the EPAS MASTER appliance and communicated to the consultants performing the installation. This is required during the datacenter installation/access.
Firewall access	Scope: EPAS MASTER For connecting to the EPAS management console, which will be used for the training, the (minimum) firewall/access rules should be in place: Source: Training office/conference room (customer's workstation) Target: EPAS MASTER IP address Allowed ports (TCP): 80 443 8080 8443
Firewall access (Optional)	Scope: EPAS MASTER For connecting the EPAS MASTER to different components (e.g. DNS, SMTP). Components are optional, and port numbers specified are defaults. Source: EPAS MASTER IP address Target: External Service(s) IP address(es) Allowed ports: 53 UDP (DNS), 25 TCP (SMTP), 123 UDP (NTP)

Target System (Microsoft Active Directory) requirements

For auditing Microsoft® Active Directory environments, the following requirements should be in place:

Requirement	Notes
Firewall access (Generic)	Scope: Active Directory – password audit (regardless of version) Source: EPAS MASTER IP address Target: Active Directory Domain Controller (1 DC) Allowed ports (TCP): 135 139 445 Allowed ports (UDP): 137 138 Note: the EPAS does not require a connection to the primary domain controller; backup domain controllers can also be used as targets, instead of the PDC. In this scenario, the only requirement is that the target DC is a read-write domain controller (standard).
Firewall access (2008R2 or newer)	Scope: Active Directory (2008R2 or newer) – password audit Source: EPAS MASTER IP address Target: Active Directory Domain Controller (1 DC) Allowed ports (TCP): 49152 to 65535 (DCOM/RPC port range)
Firewall access (2003)	Scope: Active Directory (2003) – password audit Source: EPAS MASTER IP address Target: Active Directory Domain Controller (1 DC) Allowed ports (TCP): 1025 to 5000 (DCOM/RPC port range)
System Credentials	Scope: Active Directory – password audit Requirement: Domain Administrator or equivalent Note: the credentials are required to retrieve an initial set of profile information for the password audit. The credentials can be disabled afterwards.

Deployment Scenarios

The following scenarios are proposed as part of an EPAS deployment. The scenarios are purely theoretical, based on previous installations or proof-of-concept deployments of EPAS, and provide a guideline for deployment

Scenario 1: EPAS MASTER in an isolated zone

The EPAS MASTER is deployed within a completely isolated network area. In this scenario, the EPAS cannot communicate with any systems within a target environment without explicit firewall rules to allow communication to target systems.

The advantages are complete separation from any network areas deployed in the environment. As EPAS updates are applied manually by the EPAS administrator, from the management interface, this deployment does not affect the functioning of EPAS.

The disadvantage of this approach is that it can become cumbersome to implement in environments with many target systems; the approach is normally not recommended for productive usage, as to audit each system, it is required to open firewall rules between EPAS and the audited target, as detailed in the **Target System Requirements** section.

This is the default deployment for proof-of-concept installations. For productive usage, the second scenario is more suitable.

Scenario 2: EPAS MASTER in the management zone

The EPAS MASTER is deployed within the management network area. In this scenario, the EPAS can communicate with systems within the same network area, so defining multiple targets within the management network does not require additional firewall configuration.

As the management network(s) are normally privileged when it comes to network access to other less-privileged zones, this scenario has the advantage that most target system configurations will not require opening additional firewall rules.

Given the security hardening of the appliance, as well as the fact that the EPAS does not degrade the security level of the information stored and collected, this is the ideal target deployment for productive environments.

Data Encryption – Trusted Computing

The data which is stored on the EPAS appliance is encrypted at all times. The encryption key is stored During the assembly process of the EPAS hardware appliances, all the data is encrypted (AES-CBC-ESSIV) using a unique 256-bit random key, which is then stored on the TPM chip of the appliance.

The encryption key is “sealed” to the unique hardware configuration of the EPAS unit. This process is built on the Trusted Computing technology, providing security and hardening of the hardware appliance. The encryption key is unsealed at the boot time automatically if no hardware modifications or boot software tampering has been detected; if any hardware or boot software modifications have taken place, the key cannot be unsealed and the entire content of the internal storage is permanently lost.

The same can be achieved by destroying the TPM module, which is the normal EPAS unit recycling procedure. The exportable backups are not affected by the data loss (they can be imported and restored on a new EPAS hardware unit).

After the hardware is sealed, the configuration data and all other information on the respective machine is only available to that exact hardware unit. This measure is taken as an additional hardening step for the appliance, to protect the customer data and to protect the EPAS internal software against unauthorized access. Any attempt to modify, remove or tamper with the hardware unit will render the data on the unit unreadable. Only the original hardware is able to read any data on the hard drive. Therefore, it is impossible to provide any disaster recovery or data recovery if the EPAS hardware fails to boot the operating system.