

Best Practices Guide



TABLE OF CONTENTS

5

Overview

- 1.1 About Access Manager Plus
- 1.2 About the guide

7

Recommended system configuration

- 2.1 Minimum system requirements

9

Installation

- 3.1 Windows vs. Linux
- 3.2 Backend database
- 3.3 Secure the master key
- 3.4 Take control of the database credentials

13

Server and environmental settings

- 4.1 Server hardening
- 4.2 Use a dedicated service account
- 4.3 Configure a bound IP address for the webserver
- 4.4 Restrict webserver access by blacklisting or whitelisting IP addresses

16

User onboarding and management

- 5.1 Leverage AD/LDAP/Azure AD integration for authentication and provisioning
- 5.2 Disable local authentication
- 5.3 Use two-factor authentication
- 5.4 Assign user roles based on job responsibilities
- 5.5 Create user groups
- 5.6 Remove the default user accounts

20

Data population and management

- 6.1 Adding connections: Choose a convenient method
- 6.2 Remove unmanaged, unwanted, and unknown privileged accounts
- 6.3 Leverage the power of connection groups

23

Granular access controls

- 7.1 Make use of access control workflows
- 7.2 Require users to provide reason for retrieving passwords
- 7.3 Integrate Access Manager Plus with enterprise ticketing systems

25

Secure remote access

- 8.1 Enable users to automatically log on to remote systems without revealing passwords in plain text
- 8.2 Configure gateway settings
- 8.3 Leverage advanced settings for connections
- 8.4 Discover and configure RemoteApp for Windows servers

29

Privileged access to third parties

- 9.1 Manage third-party access to corporate systems

31

Data center remote access

10.1 Avoid circulating jump server credentials

33

Session management and monitoring

11.1 Monitor critical sessions in real time

11.2 Record every privileged session

11.3 Regularly purge recorded sessions

36

Auditing

12.1 Facilitate regular internal audits

12.2 Keep a tab on select activities with instant alerts

12.3 Opt for daily digest emails to avoid inbox clutter

12.4 Send syslog messages and SNMP traps to your event and network management systems

12.5 Purge audit records

40

Data redundancy and recovery

13.1 Set up disaster recovery

42

Maintenance

14.1 Keep your installation updated

14.2 Choose your maintenance window wisely

14.3 Look for security advisories

14.4 Moving the Access Manager Plus installation from one machine to another

C1

Overview

1.1 About Access Manager Plus

ManageEngine Access Manager Plus is a web-based privileged session management software that regulates access to remote systems through secure channels from a unified console. With comprehensive auditing capabilities, it offers total visibility into all privileged access usage, and lets enterprises manage privileged user sessions in real time, shutting the door on access misuse. It also helps prove compliance with regulations like PCI DSS, GDPR, NERC CIP, and SOX.

1.2 About the guide

This guide describes the best practices for getting started with Access Manager Plus in an enterprise network. Coming from our experience of helping organizations around the world deploy the software successfully, this guide offers instructions to IT security administrators to set up an efficient and streamlined privileged session management software. These best practices can be adopted during all stages—product installation, configuration, deployment, and maintenance—and they are explained below with special focus on data security, scalability, and performance.

The logo consists of the characters 'C' and '2' in a bold, yellow, sans-serif font. The 'C' is a simple outline, and the '2' has a thick, blocky appearance with a small horizontal bar at the bottom right.

**Recommended system
configuration**

2.1 Minimum system requirements

Before installing Access Manager Plus, you need to evaluate the system configuration. The minimum system requirements to run Access Manager Plus can be found [here](#).

In general, the performance and scalability depends on the following factors:

- Number of users and groups
- Number of active connections
- Frequency of remote connections
- Number of scheduled tasks
- Storage space (free disk space available in hard drive)

Based on the above factors, the following system settings are recommended for small, medium, and large enterprises:

Hardware Requirements

| Organization Size | Processor | RAM | Hard Disk |
|--|------------------------------------|-------|--|
| Small (<1000 servers, <500 keys and <500 user) | Dual Core / Core2 Duo or above. | 4 GB | <ul style="list-style-type: none"> • 200 MB for product • 10 GB for database |
| Medium (<5000 servers, <1000 keys and <1000 users) | Quad Core or above. | 8 GB | <ul style="list-style-type: none"> • 500 MB for product • 20 GB for database |
| Large (>5000 servers, >1000 keys and >1000 users) | Octa Core or above | 16 GB | <ul style="list-style-type: none"> • 1 GB for product • 30 GB for database |

Note:

We also recommend that you install Access Manager Plus on a dedicated, hardened, high-end server for superior performance and security.

C3

Installation

3.1 Windows vs. Linux

Access Manager Plus can be installed on either Windows or Linux. Although the software runs equally on both the platforms, installing on Windows provides an inherent advantage on Active Directory integration:

Active Directory (AD) integration:

A Windows installation of Access Manager Plus can be directly integrated with AD/Azure AD to import users and groups. Moreover, users who have logged into their Windows system using the domain account credentials can leverage single sign-on (SSO) using the Windows security protocol NT LAN Manager (NTLM) to automatically log in to Access Manager Plus

3.2 Backend database

Access Manager Plus provides backend support for PostgreSQL database and MS SQL server. By default, the product comes bundled with PostgreSQL database, which is ideal for small- and medium-sized businesses. Meanwhile, for large businesses, we highly recommend you use MS SQL server as your backend for better scalability, performance, clustering, and disaster recovery.

If you are using MS SQL server as your backend, we suggest you follow these practices:

- Access Manager Plus can communicate with the MS SQL server only over SSL, with a valid certificate configuration. Therefore, we recommend that you have a dedicated SQL instance for Access Manager Plus to avoid any conflicts or disruptions with existing databases.
- While using the MS SQL server as your backend, a unique key is auto-generated for database-level encryption and, by default, this key will be stored in the directory, in a file named <masterkey.key>. We recommend that you move the key file to a different location to protect it from unauthorized access.
- Use Windows authentication while configuring MS SQL server as your backend rather than using an SQL local account.
- We recommend you use the same domain account to run both Access Manager Plus server and MS SQL server, so that you can run SQL service and SQL agent services.
- The force encryption option should be enabled to allow all clients to connect to this SQL instance. When this is done, all client-to-server communication will be encrypted and clients that cannot support encryption will be denied access.
- Disable all protocols other than TCP/IP in the machine where MS SQL server is running.
- Hide this SQL instance to prevent it from being enumerated by other tools and disable access to this database for all other users except Access Manager Plus's service account.
- Set up firewall rules to allow access only for the required ports in the machine where the MS SQL server is running.

3.3 Secure the master key

Access Manager Plus uses AES-256 encryption to secure passwords and other sensitive information. The key used for encryption (*amp_key.key*) is auto-generated and unique for every installation. By default, this key will be stored in the `<AMP_HOME/conf>` directory, in a file named `<amp_key.key>`. The path of this key needs to be configured in the *manage_key.conf* file present in the `<AMP_Installation_Folder>/conf` directory. Access Manager Plus requires this folder to be accessible with necessary permission to read the *amp_key.key* file when it starts up every time. After a successful start-up, it does not need access to the file anymore and so the device with the file can be taken offline. We highly recommend you move this key to a different secure location and lock it down by providing read access only to Access Manager Plus's service account. Also, update this remote path in the *manage_key.conf* file so that the product can read the encryption key during start up. You can also secure this key by storing it in a USB drive or a disk drive. For extreme security, create script files to copy this key into a readable location and then destroy the copy upon service start up.

3.4 Take control of the database credential

Apart from AES encryption, the Access Manager Plus database is secured through a separate password, which is auto-generated and unique for every installation. This database password can be securely stored in Access Manager Plus itself. However, we recommend you store the password in some other secure location accessible to the product server. By default, the database information, such as the JDBC URL, log in credentials, and other parameters, will be stored in a file named *database_params.conf*, which is present in the directory. Although the database is configured to not accept any remote connections, we recommend you move this file to a secure location, restrict access, and make it available only for Access Manager Plus's service account. However, you will have to copy the file back to the original location (i.e., to `<AMP_Installation_Folder>/conf`) while performing the application upgrade. If you place the *database_params.conf* file outside the Access Manager Plus installation folder, you need to specify the location along with the filename in `\conf\wrapper.conf` file (for Windows) or `\conf\wrapper_lin.conf` file (for Linux). Note that the service cannot be started if the entire location is not specified here.

- The path of this file is configured in the `"wrapper.conf"` file present in the directory. Edit this file and look for the line

wrapper.java.additional.9=-Ddatabaseparams.file.

- If you are using a Linux installation, then you will have to edit the file `"wrapper_lin.conf"` present in the directory.

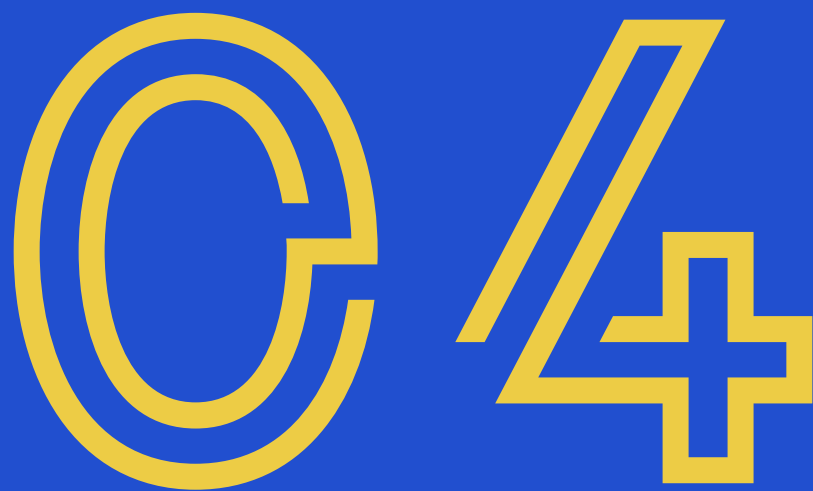
The default path will be configured as `../conf/database_params.conf`. Move the `"database_params.conf"` file to a secure location and specify its path in the above file. For example,

wrapper.java.additional.9=-Ddatabaseparams.file=\\remoteserver1\tapedrive\sharedfiles\database_params.conf.

- Save the file and restart Access Manager Plus for the change to take effect.

Note:

The above steps are applicable only for PostgreSQL and MySQL. If you are using MS SQL server as your backend, refer to section 3.2.



Server and
environmental settings

4.1 Server hardening

By default, all components required for Access Manager Plus to function are stored in the installation directory (*ManageEngine/AMP*). Therefore, we highly recommend you harden the server where Access Manager Plus is installed. Some of the basic steps you should carry out are as follows:

- Disable remote access to this server for all regular domain users in your organization using domain group policies. Restrict read permissions for all regular administrators, and provide write permissions to Access Manager Plus drive or directories for only one or two domain administrators.
- Set up inbound and outbound firewalls to protect against incoming and outgoing traffic, respectively. Using this setting, you can also specify which server ports must be opened and used to conduct various session management operations such as remote access.

4.2 Use a dedicated service account

Create a separate service account for Access Manager Plus in your domain controller. To begin using this service account, go to the service console (*services.msc*) in the server where Access Manager Plus is installed, and review the properties. Replace the configured local system account with the service account created. This same service account can also be used for importing users and resources from AD.

4.3 Configure a bound IP address for the webserver

By default, Access Manager Plus's webserver will bind to all available IP addresses of the server in which the application is installed. Due to this, Access Manager Plus will be reachable on any or all IP addresses with the configured port (9292). To restrict this, we recommend you configure the web server to bind to a single IP address and receive incoming communications from that IP address alone. The following steps can be used to configure the bound IP:

- Stop Access Manager Plus if it is running.
- Open the *server.xml* file present in the *\conf* folder.
- Search for this code snippet:

```
<Connector SSLEnabled="true" URIEncoding="UTF-8"
acceptCount="100" ciphers="TLS_RSA_WITH_AES_256_CBC_SHA,TLS_
RSA_WITH_AES_256_CBC_SHA256" clientAuth="false" debug="0"
disableUploadTimeout="true" enableLookups="false" keystoreFile="conf/server.key-
store" keystorePass="passtrix" maxHttpHeaderSize="32768" maxSpareThreads="75"
maxThreads="150"
minSpareThreads="25" port="9292" scheme="https" secure="true" server="PMP" sslProto-
col="TLS" truststoreFile="-
jre/lib/security/cacerts" truststorePass="changeit" truststoreType="JKS" useBodyEncoding-
ForURI="true"/>
```

In the above snippet, next to the value `port="9292"`, add the attribute `address="127.0.0.1"`. Replace 127.0.0.1 with the actual IP address of the server that you want to use for binding.

4.4 Restrict webserver access by blacklisting or whitelisting IP addresses

Access Manager Plus can be accessed from any client system, as long as there is connectivity. We recommend you restrict and provision only a limited number of client systems with access to Access Manager Plus. To configure IP-based restrictions, navigate to **Admin > IP Restrictions > Web Access**. The IP restrictions can be set at various levels and combinations, such as defined IP ranges or individual IP addresses. You can choose to allow web access to specific IP ranges and addresses or alternatively, restrict access by adding them to the blocked IP addresses field.

The logo consists of the characters 'C' and '5' in a bold, yellow, sans-serif font. The 'C' is a simple outline, while the '5' has a thick, blocky appearance with a horizontal bar at the top. The background is a solid blue color with large, dark blue chevron shapes pointing towards the center.

User onboarding
and management

5.1 Leverage AD/LDAP/Azure AD integration for authentication and provisioning

Integrating Access Manager Plus with AD, Azure AD, or any LDAP-compliant directory can be very useful, as it provides the following benefits:

User provisioning or deprovisioning:

With AD/LDAP/Azure AD integration, adding a user in Access Manager Plus is quick and easy. Once integrated, you can directly import the user profiles and groups or organizational units (OUs) from your directory to Access Manager Plus. Moreover, user account provisioning in the product becomes a simple process. For instance, if you import an existing OU of “Database Administrators” from your directory to Access Manager Plus, you can easily allocate the database passwords to that imported group. On top of this, you can enable synchronization while integrating Access Manager Plus with your directory so that any change, such as a user newly added or moved around between OUs in your directory, will automatically reflect in Access Manager Plus. Synchronizing Access Manager Plus with your directory will also keep you notified when a user is permanently deleted from the corresponding user directory. Access Manager Plus disables and locks such user accounts, and notifies you of the same through an email and alert notification, upon which you can choose to either delete those accounts or reactivate them.

The screenshot shows the 'Active Directory Configuration' page in the Access Manager Plus Admin console. The page is titled 'Active Directory Configuration' and contains the following steps:

- 1 Import Users from Active Directory**: Users from the selected domain are added to the Access Manager Plus database. During subsequent imports only the new user entries in AD are added to the local database. There is an option to import organizational units (OUs) or user groups, in which case AMP user groups are automatically created with the name of the corresponding OU or AD user group. The AMP user database is automatically synchronized with the AD, if needed. Buttons: View Synchronization Schedules, Import Now.
- 2 Specify Appropriate User Roles**: All the users imported from AD directory will be assigned the role set as default by the administrator, if no default user role has been specified, the role 'Password User' will be automatically assigned for the imported users. For appropriate users, change their roles as required. Button: Assign Roles Now.
- 3 Enable Active Directory Authentication**: Enabling this will allow your users to use their AD domain password to login to Access Manager Plus. Note that this scheme will work only for users who have been already imported to the local database from AD. Current Status: Disabled. Button: Enable.
- 4 Enable Single Sign On**: Users who have logged into the Windows system using their domain account need not separately sign in to Access Manager Plus, if this setting is enabled. For this to work, AD authentication should be enabled and the corresponding domain user account should have been imported into AMP. The IE browser supports this by default and follow these instructions to get this working in Firefox. Current Status: Disabled. Button: Enable.

5.1 Configuring AD settings for user onboarding and authentication.

AD authentication:

Another benefit is that you can leverage your directory's respective authentication mechanism and provide your users with single sign-on (SSO) options. Once you activate this option, users will be automatically authenticated into Access Manager Plus (using NTLM-based authentication) as long as they have already logged in to the system with their directory credentials. Using AD credentials for Access Manager Plus authentication ensures that login passwords are not stored locally in Access Manager Plus, since users will be directly authenticated from the directory.

Note:

Apart from AD/Azure AD/ LDAP authentication, Access Manager Plus also supports:

- Any RADIUS (Remote Authentication Dial-In User Service)-based authentication
- Smart card public key infrastructure (PKI)/certificate authentication
- Security Assertion Markup Language (SAML)-based SSO (including Okta, Azure AD, and Active Directory Federation Services (ADFS))

5.2 Disable local authentication

After integrating Access Manager Plus with your AD/Azure AD/LDAP-compliant directory, we advise you disable local authentication and let users log on to Access Manager Plus using their AD/LDAP/Azure AD credentials. To disable local authentication, navigate to **Admin > Server Settings > General Settings > User Management**, and enable the checkbox **Disable local authentication**. However, if you have configured a local Access Manager Plus account for break-glass purposes, you cannot disable local authentication. In such cases, if you still want to have only AD/LDAP/Azure AD authentication, we recommend you disable the **"Forgot Password"** option in the same section (option used to reset the local authentication password for all users in Access Manager Plus). Disabling this option will ensure users can log in to Access Manager Plus using only their AD/LDAP/Azure AD credentials, even if local authentication is enabled.

5.3 Use two-factor authentication

An additional protective layer of user authentication ensures that only the right people have access to sensitive resources. Access Manager Plus provides multiple options for configuring a second level of authentication before providing access to the product's web interface. The second factor options are: PhoneFactor, RSA SecurID tokens, Duo Security, Google Authenticator, unique passwords through email, any RADIUS-compliant authentication, Microsoft Authenticator, Okta Verify, and YubiKey. It is highly recommended that you configure two-factor authentication for your users.

5.4 Assign user roles based on job responsibilities

After adding users, assign them proper roles. Access Manager Plus has two predefined user roles: Administrator and Standard User. The administrator role should be restricted only to the handful of people who need to perform user onboarding and management. Apart from the default roles, Access Manager Plus also enables you to add custom roles from the scratch. [Click here](#) to learn more about custom roles. For additional security, a new custom role added by an administrator has to be approved by another administrator.

5.5 Create user groups

Organize your users into specific groups—for example, Windows administrators, Linux administrators, technicians, etc. User grouping helps improve efficiency when sharing resources and delegating passwords. If you've integrated Access Manager Plus with AD/LDAP/Azure AD, you can import user groups directly from the directory, and use the same hierarchical structure.

5.6 Remove the default user accounts

For security reasons, we highly recommend that you delete the default user accounts like the admin and guest accounts in Access Manager Plus, after you have added one or more users with the administrator role.



**Data population and
management**

6.1 Adding connections: Choose a convenient method

The first step to getting started with access management in Access Manager Plus is to add remote target systems in as “Connections” to launch secure remote connections. The quickest and most convenient way to do this is automated discovery of Windows and Linux remote systems.

6.1.1 Automated discovery of Windows connections

The other ways are manual addition and CSV import. Use the CSV import feature if you’ve used another tool before switching to Access Manager Plus, or have your resource details stored in spreadsheets.

6.1.2 Manual addition of an SSH connection

6.2 Remove unmanaged, unwanted, and unknown privileged accounts

When you use the auto-discovery feature to inventory a Windows or Linux connection on your network, Access Manager Plus will, by default, add every single account associated with them as a connection. Some accounts may be unmanaged, unwanted, or orphaned. For instance, when you add a Windows connection, all guest accounts will also be fetched.

From a security perspective, such accounts should be identified and deleted to avoid any unforeseen vulnerabilities in the future. We recommend you keep the number of privileged accounts at a minimum. Moreover, dumping unwanted accounts can clutter the database and make data organization a daunting task. Therefore, it's ideal to remove these unwanted accounts in the target machine itself before running auto-discovery in Access Manager Plus.

6.3 Leverage the power of connection groups

Access Manager Plus lets you create connection groups to facilitate bulk edits and bulk configuration of settings to all the connections associated with that particular group. Connection groups can also serve as a means to combine similar types of connections under one umbrella, and view them separately from the Connections tab.

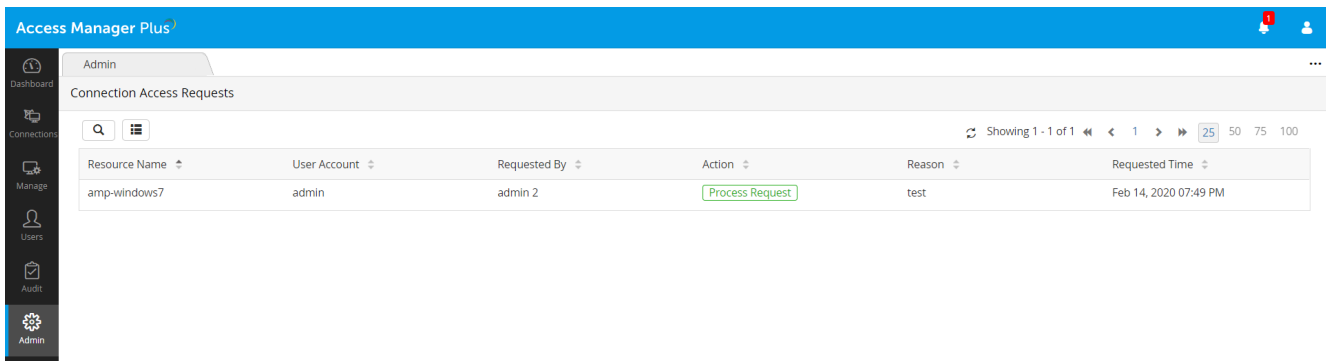
This feature provides you the flexibility to consolidate connections that satisfy certain criteria into a single group. Once a connection group is created, use the Group Action option to perform bulk setting changes on all the connections that are part of the group.



Granular access controls

7.1 Make use of access control workflows

Access control in Access Manager Plus is a request-release mechanism that doesn't allow users to access remote systems directly. Instead, users have to raise a request to the IT admin for access approval. The feature also helps you introduce various other restrictions for your resources such as time limited access and concurrency controls. We highly recommend you enable this feature for your critical resources.



7.1 Request-release mechanism in Access Manager Plus

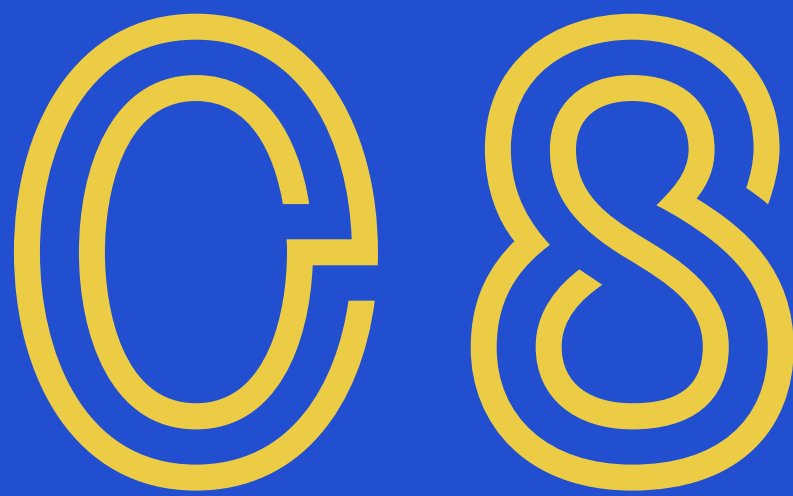
Access controls can be configured by going to **Manage > Connections > Connection Actions > Edit Connection > Enable Access Control**.

7.2 Require users to provide reason for retrieving passwords

By default, all access-related operations are captured in Access Manager Plus' audit trails, complete with timestamp and IP address details. Optionally, you can mandate users to provide a reason for remote access. These reasons will also be recorded in the audit trails, which can be used for cross-verification and validation in forensic investigations. Therefore, whenever a user tries to access a connection, we recommend you mandate that they provide a credible reason for requiring access, irrespective of whether access controls are configured. This option can be activated under **Admin > Server Settings > General Settings > Password Retrieval**.

7.3 Integrate Access Manager Plus with enterprise ticketing systems

Access Manager Plus provides the option to integrate a range of ticketing systems to automatically validate service requests related to privileged access. The integration ensures that users can access a remote system only with a valid ticket ID. In order to enable stronger remote access workflow, we suggest you integrate Access Manager Plus with your enterprise ticketing system. Currently, Access Manager Plus readily integrates with ManageEngine ServiceDesk Plus On-Demand, ServiceDesk Plus MSP, ServiceDesk Plus, ServiceNow, and JIRA. You can integrate Access Manager Plus with the ticketing systems mentioned above by navigating to **Admin > Session Settings > Ticketing System Integration**.

The image features the letters 'CS' in a large, bold, yellow, double-lined font. The background is a solid blue color with large, dark blue geometric shapes, including chevrons and arrows, pointing in various directions.

Secure remote access

8.1 Enable users to automatically log on to remote systems without revealing passwords in plain text

After you configure auto-logout options to remotely connect to the machines, Access Manager Plus allows users to establish a direct connection to the remote system with just a single click, eliminating the need to copy and paste passwords. In such cases, we recommend that you prevent users from retrieving the passwords in plain text, since it is not required. Plain text retrieval of passwords can be disabled from **Admin > Server Settings > General Settings > Password Retrieval**.

8.2 Configure gateway settings

Access Manager Plus allows you to customize gateway settings. You can edit and control the cipher suites that are used for SSL communication, set up a different port, choose SSL protocols to be used for securing remote connections initiated from the product, customize HTTP header log settings, etc. To edit the gateway settings, navigate to **Admin > Session Settings > Gateway Settings**. Apart from this, you can also refer to the *gateway.conf* file in the path `<AMP_installation_directory>\conf` for a more extensive customization and for other technical details.

Gateway Settings
✕

Gateway Port :

Session Recording : Enable Disable

SSL Protocols : TLSv1 TLSv1.1 TLSv1.2

Allowed Cipher Suites :

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA

Recording Notification : Enable Disable

Save
Reset
Cancel

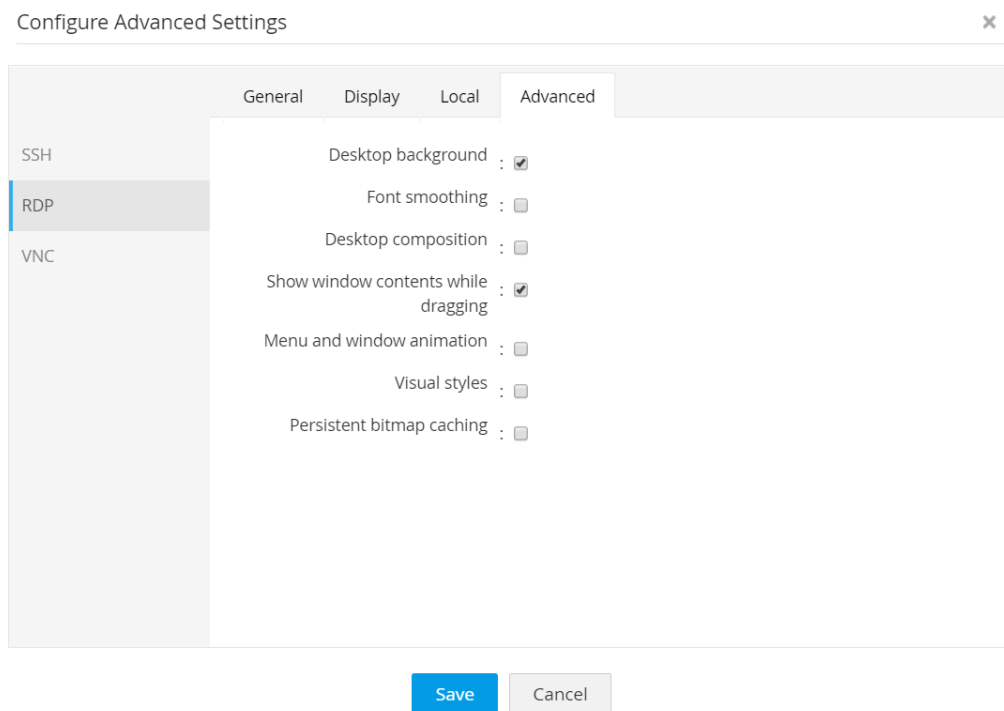
8.2 Configuring gateway settings

8.3 Leverage advanced settings for connections

Access Manager Plus offers advanced configuration settings for connections that can be customized to improve the speed and performance of the remote connections initiated from within the product. These enhancements are available for SSH, RDP, and VNC connections for centralized configuration and ease of use. All the settings changes made here will be applied locally on the remote system too. Some of the advanced settings include keyboard layout, desktop backgrounds, map drives, remote audio support, etc.

To configure these settings for a connection, click the **Actions** drop-down beside any connection name and choose **Advanced Settings**. To configure the settings in bulk, select the required connections and click **Advanced Settings** from the **More Actions** drop-down menu.

[Click here](#) to learn more about the advanced settings.



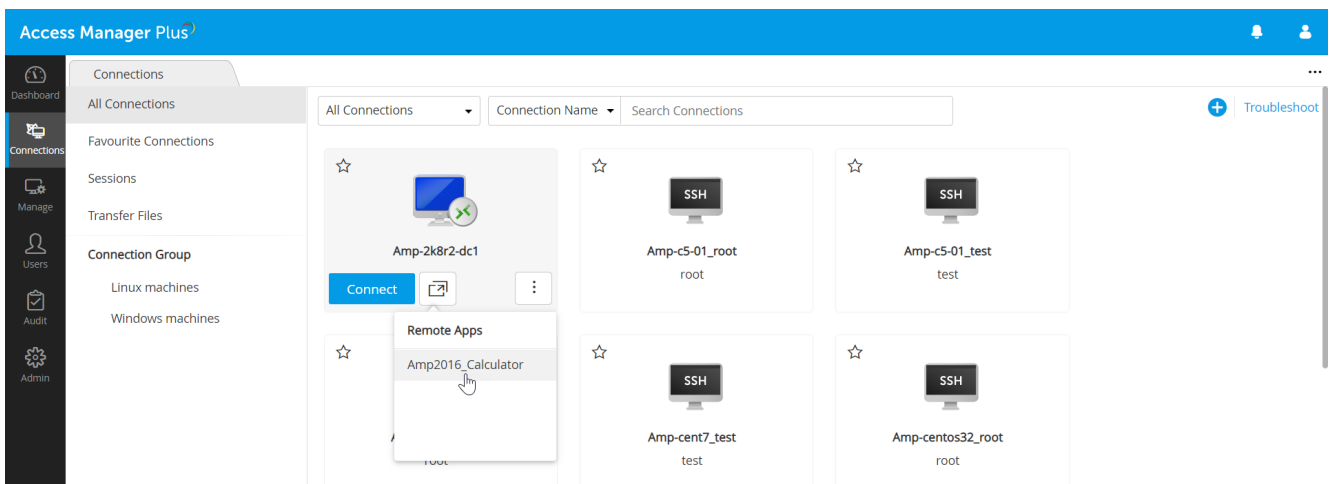
8.3 Advanced settings for RDP

8.4 Discover and configure RemoteApp for Windows servers

Note:

You need to install the required RemoteApps on the remote target servers to use this feature.

Apart from launching direct connections to remote systems, you can allow users to connect to particular apps that are configured as RemoteApps in the target systems. You can either automatically discover RemoteApps configured in the target Windows systems, or manually add them in Access Manager Plus. Configuring RemoteApps for Windows connections makes managing privileged RDP sessions more secure, as it limits a user's access to the particular application that is launched, instead of the entire remote desktop. For example, consider that if you've whitelisted an app, say SQL Studio, for a particular user. Now, when the user launches a session, it will automatically open SQL Studio and the user can only use that application. They cannot see the taskbar or navigate to any other area or perform any other operation other than using SQL Studio.



8.4 Connecting to a RemoteApp during an RDP



**Privileged access to
third parties**

9.1 Manage third-party access to corporate systems

Most often, third parties such as contractors, consultants, and vendors require access to corporate IT resources for various contractual duties and other business needs. When you provide privileged access to a third party, we always recommend you provision them only with temporary access, restricted with time stipulations and minimum necessary privileges. On top of that, here are a few more suggested practices to follow while sharing critical information with third parties:

- Since contractors connect remotely to your resources, add all your third parties as users in Access Manager Plus and require them to establish direct sessions to target systems only through Access Manager Plus.
- After configuring auto-logon for the resource, the best practice approach is to share the login credentials without displaying the passwords in plain text.
- Also, configure access control workflows for such resources. This helps implement time limits for access to the systems.
- Oversee sessions regularly to detect any trace of malicious behavior and instantly adopt remediation measures.
- When you end a contract with a vendor, immediately execute password resets for all the connections that they had access to—either manually, or with the help of a password management tool—and update the connection passwords in Access Manager Plus.

The logo consists of the characters '10C' in a bold, yellow, sans-serif font. The '1' is a simple vertical bar with a small horizontal top bar. The '0' is a thick, rounded ring. The 'C' is a thick, rounded shape with a small gap at the bottom right. The background is a solid blue color with large, dark blue, stylized arrow shapes pointing outwards from the center.

Data center remote
access

10.1 Avoid circulating jump server credentials

Normally, connecting to remote data center resources is a lengthy process, since direct access is restricted from a security perspective. To overcome these access barriers, users usually hop through jump servers before ultimately connecting to the target device. This process of multiple hops requires users to provide separate credentials for each jump server to launch a data center connection. Circulating all the credentials among users to facilitate a remote data center connection is not a secure practice. Instead, you can use the landing server configuration feature to force your users to connect to data centers only through Access Manager Plus. The application provides secure, one-click, and automated access to the data center resources via RDP and SSH jump servers (single jump server for Windows and multiple jump servers for Linux). This eliminates the need for manual authentication at every hop. Access Manager Plus lets you to store all the jump server credentials in a single, centralized console.



Session management and monitoring

11.1 Monitor critical sessions in real time

Access Manager Plus offers session shadowing, which can be used to establish dual controls on privileged sessions. Use this feature to monitor remote sessions in real time and supervise user activity. Dual controls are helpful to provide remote assistance and thwart malicious activities. If you are an admin, you can track critical sessions launched from the application by joining active sessions and observing concurrently, without affecting the end user. You can join an active session by navigating to **Connections > Sessions > Join**. When a user launches a remote session, multiple users can join the same session and collaborate. This can be done by navigating to **Connections > Sessions**, and clicking on **Collaborate** beside the required active session. Session collaboration will be especially useful for troubleshooting as all the users will be able to control the mouse cursor and work collaboratively in the same RDP or SSH session. In case any suspicious activity is detected, you can terminate the session immediately to avoid any misuse of privileged access. This can be done by navigating to **Audit > User Sessions**, and clicking on **Terminate** beside the required session.

11.2 Record every privileged session

By default, Access Manager Plus records all RDP, VNC, SSH, and SQL sessions launched from the application. We recommend that you configure session recording for all the privileged sessions, and customize the external storage location by navigating to **Admin > Session Settings > Session Recording**. All the recorded sessions will be displayed under **Connections > Sessions > Completed**. You can trace sessions using any detail such as the name of the connection, the user who launched the session, or the time at which the session was launched.

Session Recording
✕

Record RDP sessions

Record VNC Sessions.

Record SSH and SQL Sessions.

External Location for Recorded Sessions

Directory for storing recorded sessions :

Backup Directory for storing recorded sessions :

Purge Recorded Sessions

Purge recorded sessions that are more than days old. ⓘ

Save
Cancel

Privileged sessions launched from AMP can be recorded, archived and played back to support forensic audits. The above settings enable recording of RDP, VNC, SSH and SQL sessions in AMP. This can be disabled anytime.

11.2 Configuring session recording for RDP, VNC, SSH and SQL connections

11.3 Regularly purge recorded sessions

If your organization is large, with a comprehensive range of resources for which session recording is enabled, the recorded sessions will naturally grow at a faster rate. If you do not need recordings that are older than a specified number of days, we recommend you purge them to keep the disk space free. You can also store these recordings in the local drive, so they can be moved elsewhere. If you want to delete a selective session or the chat history of a particular session, you can do so by navigating to **Admin > Session Settings > Session Recording > Purge Recorded Sessions**. To purge the records that are older than a specified number of days, enter the number under **Purge recorded sessions that are more than __ days old**. You can disable purging by leaving the text field empty or by entering “0” as the value.

A large, stylized number '12' in a bright yellow color. The '1' is a simple vertical bar with a small hook at the top. The '2' is a thick, rounded shape with a curved top and a horizontal base. The background is a solid blue color with large, faint, dark blue arrow-like shapes pointing outwards from the center.

Auditing

12.1 Facilitate regular internal audits

Use Access Manager Plus' audit trails to instantly record all events around privileged account operations, user logon attempts, scheduled tasks, and completed tasks. With these data, you can facilitate regular internal audits and forensic investigations, easily discovering who accessed what resource, where, and when.

| Connection Name | User Account | Operated By | IP Address | Time Stamp | Operation Type | Username |
|-------------------|--------------|-------------|-----------------|-----------------------|------------------|----------|
| amp-win8 | N/A | admin | fe80:0:0:0:e... | Feb 14, 2020 05:56 PM | Connection Added | N/A |
| amp-win10 | N/A | admin | fe80:0:0:0:e... | Feb 14, 2020 05:56 PM | Connection Added | N/A |
| amp2k16 | N/A | admin | fe80:0:0:0:e... | Feb 14, 2020 05:56 PM | Connection Added | N/A |
| amp-win10-64-2 | N/A | admin | fe80:0:0:0:e... | Feb 14, 2020 05:56 PM | Connection Added | N/A |
| amp-2k8r2-dc1 | N/A | admin | fe80:0:0:0:e... | Feb 14, 2020 05:56 PM | Connection Added | N/A |
| AMP-U1464-1_root | N/A | admin | fe80:0:0:0:e... | Feb 14, 2020 05:56 PM | Connection Added | N/A |
| AMP-U1464-1_test | N/A | admin | fe80:0:0:0:e... | Feb 14, 2020 05:56 PM | Connection Added | N/A |
| amp-centos32_root | N/A | admin | fe80:0:0:0:e... | Feb 14, 2020 05:56 PM | Connection Added | N/A |
| amp-centos32_test | N/A | admin | fe80:0:0:0:e... | Feb 14, 2020 05:56 PM | Connection Added | N/A |
| amp-cent7_root | N/A | admin | fe80:0:0:0:e... | Feb 14, 2020 05:56 PM | Connection Added | N/A |
| amp-cent7_test | N/A | admin | fe80:0:0:0:e... | Feb 14, 2020 05:56 PM | Connection Added | N/A |
| amp-centos6_root | N/A | admin | fe80:0:0:0:e... | Feb 14, 2020 05:56 PM | Connection Added | N/A |

12.1 Connection-based audit trails in Access Manager Plus

12.2 Keep a tab on select activities with instant alerts

Access Manager Plus also lets you send instant email notifications to chosen recipients when certain events take place. This option is very handy to stay constantly updated on what your users are doing. We recommend you configure alerts for important operations such as new user addition, connection deletion, and so on. Email alerts at the operational level can be enabled by going to **Audit > Connection Audit (for example) > Audit Actions > Configure Audit**.

12.3 Opt for daily digest emails to avoid inbox clutter

If you have enabled alerts and updates for a number of connections, your inbox may overflow with notification emails. In case this occurs, you can choose to receive a daily digest email at the end of each day with a consolidated list of notifications, if hourly updates are not a priority.

12.4 Send syslog messages and SNMP traps to your event and network management systems

If you use a third-party SIEM tool in your organization, you can integrate Access Manager Plus with the tool to send syslog messages for the various events that occur during the operation of Access Manager Plus. You can do this by navigating to **Admin > Session Settings > SNMP Traps / Syslog Settings**. You can control the specific events for which notifications should be raised from **Audit > Configure Audit**.

SNMP Trap / Syslog Settings x

You can configure AMP to send SNMP traps and/or Syslog messages to other management systems, for the various events that occur during the operation of AMP. You can control the specific events for which notifications should be raised from Audit -> Configure Audit and Resource Groups -> Password Actions.

SNMP Trap Receiver Syslog Collector

Collector Hostname : 🔊 ?

Port : ?

Protocol : ?

Facility Name : ?

A RFC-3164 compliant Syslog message will be generated and sent to the configured host and port, using the chosen protocol (TCP or UDP). Default facility name will be AUTH, but you can change it to any of the unassigned facility name form the pick list.

The format of the Syslog message sent form AMP will be :
 [LOGGED_IN_USERNAME:IPADDRESS] [OPERATION_TYPE] [OPERATED_TIME] [STATUS_OF_OPERATION] [AMP_SERVER_NAME]
 [RESOURCE_NAME:ACCOUNT_NAME:REASON].

Ex: admin:127.0.0.1 Account_Added 2009/12/23 11:39:00 Success amp_test windows-server1:account1:Testing

12.4.1 Configuring syslog messages

Optionally, you can also integrate your network management tool with Access Manager Plus to receive SNMP traps. This will help you acquire a holistic view of privileged access, along with overall network activity, from a central location.

SNMP Trap / Syslog Settings x

You can configure AMP to send SNMP traps and/or Syslog messages to other management systems, for the various events that occur during the operation of AMP. You can control the specific events for which notifications should be raised from Audit -> Configure Audit and Resource Groups -> Password Actions.

SNMP Trap Receiver Syslog Collector

Receiver Hostname : 🔊 ?

Port : ?

SNMP Community : ?

A SNMP v2c trap will be sent to the configured host and port number. The varbinds include the resource name, account name, username who operated, IP address from which the user operated, date and time and the reason of the operation that resulted in the event. See [MANAGEENGINE-AMP-MIB](#) for more details.

12.4.2 Configuring SNMP traps

12.5 Purge audit records

Naturally, when each and every operation is audited, the audit records grow at a faster rate. If you do not need audit records older than a specified number of days, you can purge them. This can be configured by navigating to **Audit > Connection Audit (for example) > Audit Actions > Configure Audit > Purge Connection Audit Records**. By default, the purge option will be disabled with the days set to zero (0).

13

Data redundancy and recovery

13.1 Set up disaster recovery

Data stored in Access Manager Plus' database is of critical importance. In the unlikely event of a production setup glitch, all data could be lost. So, disaster recovery is essential. The application provides provisions for both live data backup and automated periodic backups through scheduled tasks. Choose the method that suits your organization best. Also, ensure that the configured destination directory for the backup is in a secure remote location.

A stylized yellow graphic consisting of the number '1', the number '4', and a plus sign '+'. The '1' is a simple vertical bar with a small notch at the top. The '4' is formed by a diagonal line and a horizontal line. The plus sign is a simple cross. The entire graphic is rendered in a bright yellow color against a blue background.

14+

Maintenance

14.1 Keep your installation updated

The Access Manager Plus team regularly releases upgrade packs containing enhancements and fixes. Ideally, major upgrades are released once a quarter, while minor upgrades may be announced once every month. These upgrade packs will also contain updates for the Tomcat webserver, PostgreSQL database, and JRE that come bundled with the product. To keep your Access Manager Plus installation properly maintained for optimum performance, we recommend you download and apply upgrade packs for Access Manager Plus as and when they are released.

Updating the Windows OS where Access Manager Plus is installed:

When you have Windows patches to install in the Access Manager Plus server, follow the following steps:

1. Open Services console (services.msc) and stop the Access Manager Plus service.
2. [Take a copy](#) of the entire Access Manager Plus directory and store in any other machine as a backup. If the server is a virtual machine, just take a snapshot.
3. Now, update Windows OS. You can refer to [this documentation](#) for guidance.

14.2 Choose your maintenance window wisely

In order to apply upgrade packs, Access Manager Plus has to be temporarily stopped. Therefore, we highly recommend you schedule the maintenance window during weekends or non-business hours. If you cannot avoid carrying out an upgrade during work hours, you can alert your users before the upcoming maintenance operation.

14.3 Look for security advisories

If any security vulnerabilities are discovered in the product, fixes are immediately provided through upgrade packs. A security advisory is also sent to the customer email address that you have registered with us. Keep an eye on that email address to ensure you do not miss any advisories from us. Whenever you receive one, act as advised in the email.

14.4 Moving the Access Manager Plus installation from one machine to another

To move the Access Manager Plus installation from one machine to another, follow the procedure detailed below:

1. Stop Access Manager Plus service from the services console if it's running.
2. Copy the entire Access Manager Plus installation folder from one machine to another.
3. Install Access Manager Plus on the new machine to run as service. In this option, you will not be able to uninstall the program through Windows, or add or remove the programs console. If you want to re-install anytime, just delete the entire installation folder.

For more information, refer to [this section](#) of our help documentation.

Note:

Do not remove the existing installation of Access Manager Plus until you have ensured the new installation works fine. This ensures you will have a valid backup ready, in case you need to overcome disasters or data corruption during the move.