

IBM® Security Access Manager for Enterprise Single
Sign-On
Version 8.2.1

Policies Definition Guide



IBM® Security Access Manager for Enterprise Single
Sign-On
Version 8.2.1

Policies Definition Guide



Note

Before using this information and the product it supports, read the information in "Notices" on page 137.

Edition notice

Note: This edition applies to version 8.2.1 of IBM Security Access Manager for Enterprise Single Sign-On, (product number 5724-V67) and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 2002, 2014.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

About this publication	v	Chapter 10. Policies for Debugging Management and Control.	45
Access to publications and terminology	v	Auditing policies	45
Accessibility	viii	Troubleshooting policies	45
Technical training	viii	Temporary file policy	47
Support information	viii	Log policies	47
Statement of Good Security Practices	ix		
Chapter 1. Policies in AccessAdmin.	1	Chapter 11. Policies for Wallet and AccessAgent	49
Chapter 2. Policy legends	3	Wallet policies	49
Chapter 3. Viewing and setting policy priorities	5	AccessAgent policies	56
Viewing policy priorities	5	Display policies	57
Setting policy priorities	5	ESSO GINA policies	59
Chapter 4. Policies for Authentication Factors	7	Desktop inactivity policies	63
Authentication policies	7	Lock and Unlock policies	66
Chapter 5. Policies for Password Management.	9	Smart card policies	74
Password aging policies	9	Hybrid smart card policies	75
Password change policies	11	RFID policies	79
Password strength policies	12	Fingerprint policies	85
Chapter 6. Policies for Sign up and Password Reset.	15	Terminal Server policies	88
Self-service password reset policies	15	Roaming session policies	94
Self-service registration and bypass of second factor policies	16	Log on/Log off policies	95
Sign up policies	17	Hot Key policies	101
Chapter 7. Policies for Configurable Text and Accessibility	21	Emergency Hot Key policies	105
Configurable text policies	21	Audit logging policies	107
ESSO GINA text policies	21	Background authentication policies	107
Unlock text policies	25	Network policies	108
Sign up text policies	34		
AccessAssistant and Web Workplace text policies	35	Chapter 12. Policies for AccessAssistant	111
Accessibility policy	35	AccessAssistant and Web Workplace policies	111
Chapter 8. Policies for Private and Shared desktops	37	Chapter 13. Policies for Applications and Authentication Services	115
Shared workstation policies	37	Application policies	115
Chapter 9. Policies for Citrix and Terminal Server	43	Authentication service policies	117
Lightweight mode policy	43	Password policies	117
		Authentication policies	121
		Chapter 14. Policies for ActiveCode	125
		ActiveCode policies	125
		Chapter 15. Policies for Privileged Identity Management	129
		IBM Security Privileged Identity Manager configuration policies	129

Chapter 16. Other policies	133
Chapter 17. Policy limitations in Windows 7	135
Notices	137
Glossary	141
A	141
B	142
C	142
D	143
E	144
F	144
G	144
H	144

I	145
J	145
K	145
L	145
M	145
N	146
O	146
P	146
R	147
S	147
T	149
U	149
V	149
W	150
Index	151

About this publication

IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide provides detailed descriptions of the different user, machine, and system policies that Administrators can configure in AccessAdmin. Use this guide along with the IBM® Security Access Manager for Enterprise Single Sign-On Administrator Guide.

Access to publications and terminology

This section provides:

- A list of publications in the “IBM Security Access Manager for Enterprise Single Sign-On library.”
- Links to “Online publications” on page viii.
- A link to the “IBM Terminology website” on page viii.

IBM Security Access Manager for Enterprise Single Sign-On library

The following documents are available in the IBM Security Access Manager for Enterprise Single Sign-On library:

- *IBM Security Access Manager for Enterprise Single Sign-On Quick Start Guide*, CF3T3ML
IBM Security Access Manager for Enterprise Single Sign-On Quick Start Guide provides a quick start on the main installation and configuration tasks to deploy and use IBM Security Access Manager for Enterprise Single Sign-On.
- *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*, SC23995206
IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide contains information about planning your deployment and preparing your environment. It provides an overview of the product features and components, the required installation and configuration, and the different deployment scenarios. It also describes how to achieve high availability and disaster recovery. Read this guide before you do any installation or configuration tasks.
- *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*, GI11930904
IBM Security Access Manager for Enterprise Single Sign-On Installation Guide provides detailed procedures on installation, upgrade, or uninstallation of IBM Security Access Manager for Enterprise Single Sign-On.
This guide helps you to install the different product components and their required middleware. It also includes the initial configurations that are required to complete the product deployment. It covers procedures for using virtual appliance, WebSphere® Application Server Base editions, and Network Deployment.
- *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*, GC23969204
IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide provides information about configuring the IMS Server settings, the AccessAgent user interface, and its behavior.

- *IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide*, SC23995105

This guide is intended for the Administrators. It covers the different Administrator tasks. *IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide* provides procedures for creating and assigning policy templates, editing policy values, generating logs and reports, and backing up the IMS Server and its database. Use this guide together with the *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide*.

- *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide*, SC23969404

IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide provides detailed descriptions of the different user, machine, and system policies that Administrators can configure in AccessAdmin. Use this guide along with the *IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide*.

- *IBM Security Access Manager for Enterprise Single Sign-On Help Desk Guide*, SC23995304

This guide is intended for Help desk officers. *IBM Security Access Manager for Enterprise Single Sign-On Help Desk Guide* provides Help desk officers information about managing queries and requests from users usually about their authentication factors. Use this guide together with the *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide*.

- *IBM Security Access Manager for Enterprise Single Sign-On User Guide*, SC23995005

This guide is intended for the users. *IBM Security Access Manager for Enterprise Single Sign-On User Guide* provides instructions for using AccessAgent and Web Workplace.

- *IBM Security Access Manager for Enterprise Single Sign-On Troubleshooting and Support Guide*, GC23969303

IBM Security Access Manager for Enterprise Single Sign-On Troubleshooting and Support Guide provides information about issues with regards to installation, upgrade, and product usage. This guide covers the known issues and limitations of the product. It helps you determine the symptoms and workaround for the problem. It also provides information about fixes, knowledge bases, and support.

- *IBM Security Access Manager for Enterprise Single Sign-On Error Message Reference Guide*, GC14762402

IBM Security Access Manager for Enterprise Single Sign-On Error Message Reference Guide describes all the informational, warning, and error messages that are associated with IBM Security Access Manager for Enterprise Single Sign-On.

- *IBM Security Access Manager for Enterprise Single Sign-On AccessStudio Guide*, SC23995605

IBM Security Access Manager for Enterprise Single Sign-On AccessStudio Guide provides information about creating and using AccessProfiles. This guide provides procedures for creating and editing standard and advanced AccessProfiles for different application types. It also covers information about managing authentication services and application objects, and information about other functions and features of AccessStudio.

- *IBM Security Access Manager for Enterprise Single Sign-On AccessProfile Widgets Guide*, SC27444401

IBM Security Access Manager for Enterprise Single Sign-On AccessProfile Widgets Guide provides information about creating and using widgets.

- *IBM Security Access Manager for Enterprise Single Sign-On Tivoli Endpoint Manager Integration Guide, SC27562000*

IBM Security Access Manager for Enterprise Single Sign-On Tivoli Endpoint Manager Integration Guide provides information about how to create and deploy Fixlets for AccessAgent installation, upgrade or patch management. It also includes topics about using and customizing the dashboard to view information about AccessAgent deployment on the endpoints.
- *IBM Security Access Manager for Enterprise Single Sign-On Provisioning Integration Guide, SC23995704*

IBM Security Access Manager for Enterprise Single Sign-On Provisioning Integration Guide provides information about the different Java™ and SOAP API for provisioning. It also covers procedures for installing and configuring the Provisioning Agent.
- *IBM Security Access Manager for Enterprise Single Sign-On Web API for Credential Management Guide, SC14764601*

IBM Security Access Manager for Enterprise Single Sign-On Web API for Credential Management Guide provides information about installing and configuring the Web API for credential management.
- *IBM Security Access Manager for Enterprise Single Sign-On Serial ID SPI Guide, SC14762601*

IBM Security Access Manager for Enterprise Single Sign-On Serial ID SPI Guide describes how to integrate any device with serial numbers and use it as a second authentication factor with AccessAgent.
- *IBM Security Access Manager for Enterprise Single Sign-On Epic Integration Guide, SC27562300*

IBM Security Access Manager for Enterprise Single Sign-On Epic Integration Guide provides information about the IBM Security Access Manager for Enterprise Single Sign-On and Epic integration, including supported workflows, configurations, and deployment.
- *IBM Security Access Manager for Enterprise Single Sign-On Context Management Integration Guide, SC23995404*

IBM Security Access Manager for Enterprise Single Sign-On Context Management Integration Guide provides information about installing, configuring, and testing the Context Management integrated solution in each client workstation.
- *IBM Security Access Manager for Enterprise Single Sign-On AccessAgent on Mobile Guide, SC27562101*

IBM Security Access Manager for Enterprise Single Sign-On AccessAgent on Mobile Guide provides information about the deployment and use of single sign-on on mobile devices.
- *IBM Security Access Manager for Enterprise Single Sign-On AccessAgent on Virtual Desktop Infrastructure Guide, SC27562201*

IBM Security Access Manager for Enterprise Single Sign-On AccessAgent on Virtual Desktop Infrastructure Guide provides information about setting up single sign-on support on a Virtual Desktop Infrastructure, and the different user workflows for accessing the virtual desktop.
- *IBM Security Access Manager for Enterprise Single Sign-On AccessAgent on Terminal Server and Citrix Server Guide, SC27566801*

IBM Security Access Manager for Enterprise Single Sign-On AccessAgent on Terminal Server and Citrix Server Guide provides information about the required configurations and supported workflows in the Terminal and Citrix Servers.

Online publications

IBM posts product publications when the product is released and when the publications are updated at the following locations:

IBM Security Access Manager for Enterprise Single Sign-On library

The product documentation site (http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.itamesso.doc_8.2.1/kc-homepage.html) displays the welcome page and navigation for the library.

IBM Security Systems Documentation Central

IBM Security Systems Documentation Central provides an alphabetical list of all IBM Security Systems product libraries and links to the online documentation for specific versions of each product.

IBM Publications Center

IBM Publications Center offers customized search functions to help you find all the IBM publications you need.

IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at <http://www.ibm.com/software/globalization/terminology>.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

For additional information, see "Accessibility features" in the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.

Technical training

For technical training information, see the following IBM Education website at <http://www.ibm.com/software/tivoli/education>.

Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at <http://www.ibm.com/software/support/probsub.html>.

IBM Security Access Manager for Enterprise Single Sign-On Troubleshooting and Support Guide provides details about:

- What information to collect before contacting IBM Support.
- The various methods for contacting IBM Support.
- How to use IBM Support Assistant.
- Instructions and problem-determination resources to isolate and fix the problem yourself.

Note: The **Community and Support** tab on the product information center can provide additional support resources.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Chapter 1. Policies in AccessAdmin

IBM Security Access Manager for Enterprise Single Sign-On uses policies to control the behavior of its product components.

The policies are configurable to meet specific organizational requirements. Policies have different visibilities and scopes, and are managed by different roles.

Each policy is identified by its policy ID with *pid* in the prefix. For example, `pid_wallet_authentication_option`.

System, machine, and user policies are configured in AccessAdmin.

Machine policies are typically configured in AccessAdmin. You can also configure machine policies in the Windows registry specially when the `pid_machine_policy_override_enabled` policy is set to **Yes**.

An Administrator can modify system and machine policies in AccessAdmin. A Help desk officer can view system and machine policies only. An Administrator or Help desk officer can modify user policies.

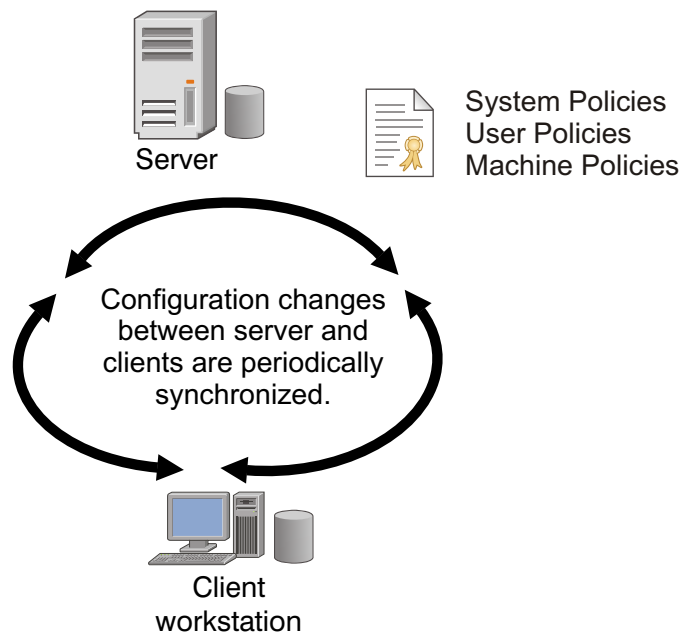


Figure 1. An overview of how different policies are synchronized between client and server in IBM Security Access Manager for Enterprise Single Sign-On.

Scope

The applicability of a policy is determined by scope.

- **System:** The policy is applicable to all users and machines.
- **User:** The policy affects a specific user.
- **Machine:** The policy affects a specific computer.

Take note of the following information.

- A policy might be defined for multiple scopes. If this policy is defined for two scopes, set a priority in case the timeout value is different for the computer and the entire system. For more information about setting policy priorities, see Chapter 3, “Viewing and setting policy priorities,” on page 5.
- Changes to these policies are propagated to the components the next time AccessAgent synchronizes with the IMS Server.
- User policy, if defined, overrides system policy.

There are three ways to edit user policies in AccessAdmin.

- Search for the user and in the page of the user, go to the appropriate policy section, and update the policy.
- Search for a group of users and in the search result, update the policy, and apply to selected users.
- Update a User Policy Template and apply it to one or more users.

Dependencies

Policies might be dependent on other policies. For example, `pid_enc_hot_key_action` is only effective if `pid_enc_hot_key_enabled` is set to **True**. If the latter is set to **False**, any setting for `pid_enc_hot_key_action` does not affect users. The dependencies are described in the later sections




User-specific policies generally override system-wide policies, but this setting also depends on the policy priority. For example, the Authentication accounts maximum policy (`pid_auth_accounts_max`) has both user and system scopes. The user scope setting is always effective if it is defined. If the user scope setting is not defined for a user, the system scope setting becomes effective.

In general, application-specific policies override authentication service-specific policies, which in turn, override general Wallet policies. The Wallet inject password entry option default policy (`pid_wallet_inject_pwd_entry_option_default`) is used when the other two policies are not defined for a particular authentication service or application. See Chapter 13, “Policies for Applications and Authentication Services,” on page 115 for more details.

Chapter 2. Policy legends

Policies can be modified only by Help desk officers and Administrators. Policies affect the behavior of the whole system and must be modified only when it is necessary. These policies must be set at deployment and followed through.

Attribute	Description
✓	Frequently used policies
Policy ID	Unique identifier of the policy.
IMS Entry	The entry in the IMS Server for System and User policies. If this column is blank, the value must be set in the registry. If not, the value indicates the name of the policy, which can be set in the IMS Server.
Description	Description of the policy, including a list of the possible behaviors that are specified by the policy. The product version that implements this policy is also indicated.
Location	Specifies the location of the policy. <ul style="list-style-type: none"> • For new policies: <ul style="list-style-type: none"> – AccessAdmin > User Policy Templates > New template > Create new policy template – AccessAdmin > Machine Policy Templates > New template > Create new machine policy template – AccessAdmin > System > System policies • For existing policies: <ul style="list-style-type: none"> – AccessAdmin > User Policy Templates > <template name> > Policy template details – AccessAdmin > Machine Policy Templates > <template name> > Policy template details – AccessAdmin > System > System policies • For registry entries: <ul style="list-style-type: none"> – Registry Editor > HKEY_LOCAL_MACHINE > SOFTWARE > IBM > ISAM ESSO
Registry	The entry in the Windows Registry (for Machine policies) or the IMS Server (for System, User, and Machine policies): <ul style="list-style-type: none"> • [DO] is [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\DeploymentOptions] • [DIMS] is [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\IMSService\DefaultIMSSettings] • [GIMS] is [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\IMSService\GlobalIMSSettings] • [T] is [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\Temp]
Type	The data type of this policy in the IMS Server or Windows Registry.
Values	Possible values of the policy. The default value is used if the policy is not specified or if the specified value is not correct.

Attribute	Description
Scope	<p>The scope of applicability of the policy.</p> <p>Values:</p> <ul style="list-style-type: none"> <li data-bbox="734 321 1154 380">•  System: Policy is system-wide <li data-bbox="734 394 1321 441">•  Machine: Policy affects only a specific machine <li data-bbox="734 457 1248 516">•  User: Policy affects only a specific user
Note	<p>The refresh frequency is indicated here. This value indicates when a policy will be effective after it is changed.</p> <ul style="list-style-type: none"> <li data-bbox="734 596 1424 684">• Refreshed on use: Policy that is read from the IMS Server or registry every time it is used. Changes, for example, are effective immediately. <li data-bbox="734 695 1424 783">• Refreshed on sync: Policy that is read from the IMS Server or registry entry only on the next synchronization with the IMS Server. <li data-bbox="734 793 1424 852">• Refreshed on logon: Policy that is read from the IMS Server or registry entry only on the next AccessAgent logon. <li data-bbox="734 863 1424 907">• Refreshed on startup: Policy that is read from the IMS Server or registry entry only on system startup.

Chapter 3. Viewing and setting policy priorities

If a policy is defined for two scopes, define which takes higher priority. Setting the priority is useful in case the timeout value for the policy is different for the two scopes. For example, if the policy priority is machine, then only the machine policy is effective.

Policies can be modified only by Help desk officers and Administrators. These policies affect the behavior of the whole system and must be modified only when it is necessary. These policies are set at deployment and followed through. Changes to these policies are propagated to clients the next time AccessAgent synchronizes with the IMS Server.

Important: Older versions of AccessAgent still use the original policy priorities, and values do not change after you upgrade the IMS Server. To change policy priorities, upgrade all installations of AccessAgent to version 8.0 or later, and then launch the command prompt.

Viewing policy priorities

View the scope and priority of a specific policy so that you can verify the implementation details of a policy.

Before you begin

Run `setupCmdLine.bat` to configure the path to the WebSphere Application Server profile where the IMS Server is installed. Set the value to `WAS_PROFILE_HOME`.

Procedure

1. Launch the Windows command prompt or Linux/Unix shell.
2. Navigate to the batch file folder. Type `<IMS installation folder>\bin`, then press **Enter**.
3. Type `managePolPriority.bat` or `managePolPriority.sh` to view the information about running the batch file, then press **Enter**.
4. Type `managePolPriority --policyId [name of policy]`, then press **Enter**. The scope and priority of a specific policy are displayed.
5. Type `exit` and then press **Enter**.

Setting policy priorities

Set the priority of a policy so that you can specify which policy is more important.

Procedure

1. Launch the Windows command prompt or Linux/Unix shell.
2. Navigate to the batch file folder. Type `<IMS installation folder>\bin`, then press **Enter**.
3. To change the scope of the policy, enter the following information.

```
managePolPriority
--policyId [name of policy]--scope [scp ims or scp machine] --templateId
[template ID]
```

The scope that is given highest priority is assigned a value of 1, the next scope is assigned with a value of 2, and so on.

Note: Provide a template ID to specify the assigned template of the machine, user, or system.

4. Press **Enter**.
5. Type `exit` to close the command prompt and then press **Enter**.

Chapter 4. Policies for Authentication Factors

This section provides a list of all policies that you must configure for different authentication factors. Examples of authentication factors are smart cards, hybrid smart cards, RFIDs, and fingerprints.

See “AccessAgent policies” on page 56 for more information about smart card, hybrid smart card, RFID, and fingerprint policies.

See the “Authentication policies” for more details.

Authentication policies

Know the different authentication policies for both user and machine scopes, where to find and set these policies, their descriptions, and their default values.

 **pid_second_factors_supported_list**

IMS Entry	Authentication second factors supported
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > Authentication Policies
Description	The second factors that are supported on this computer. This policy also controls the Wallet registration policy and imposes a constraint on the Wallet locks available for logon. Note: <ol style="list-style-type: none">1. If there is a GINA or Credential Provider installed, this policy is only updated on computer restart.2. If there is no GINA or Credential Provider installed, this policy is only updated when a new Windows session is created. For example, when the user logs on to Windows and not when the user unlocks a Windows session.3. Modifying this policy requires a computer restart to implement the changes.
Registry	
Type	String list MULTI_SZ
Values	<ul style="list-style-type: none">• RFID• Smart card• Hybrid smart card• Fingerprint
Scope	Machine
Note	<ul style="list-style-type: none">• Currently, only single value is accepted, except for simultaneous Fingerprint and RFID support.• Refreshed on startup.

 **pid_wallet_authentication_option**

IMS Entry	Wallet authentication policy
------------------	------------------------------

 **pid_wallet_authentication_option**

Location	AccessAdmin > User Policy Templates > New template > Create new policy template > Authentication Policies
Description	Authentication policy that enforces the combinations of authentication factors that can be used for logon. Note: <ol style="list-style-type: none"> 1. This policy does not enforce the authentication factors that are used for sign-up. The sign-up policy is enforced by pid_second_factors_supported_list and pid_second_factor_for_sign_up_required. 2. Smart card includes hybrid smart cards. 3. If AccessAgent is deployed without ESSO GINA but with ESSO Network Provider enabled, this policy is ignored.
Registry	
Type	Positive integer list
Values	<ul style="list-style-type: none"> • #1: Password • #2: Password + RFID • #5: Fingerprint • #6: Smart card
Scope	User
Note	<ul style="list-style-type: none"> • You can select multiple values. • All values are supported for 32-bit AccessAgent. • Only password and password+RFID are supported for 64-bit AccessAgent. • Refreshed on logon or unlock by different user, if online. • Refreshed on sync.

 **pid_mac_auth_enabled**

IMS Entry	Enable Mobile ActiveCode authentication?
Location	AccessAdmin > User Policy Templates > New template > Create new policy template > Authentication Policies
Description	Whether Mobile ActiveCode authentication is enabled for the user.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none"> • #True: Yes • #False: No (default value)
Scope	User
Note	Refreshed on use.

Chapter 5. Policies for Password Management

The Password Management policies contain all the settings to configure for passwords, such as password aging, change, and strength.

For more information:

- “Password aging policies”
- “Password change policies” on page 11
- “Password strength policies” on page 12

Password aging policies

Know the different password aging policies, where to find and set these policies, their descriptions, and their default values. Password aging policies follow the strictest or the most secure policy.



pid_enc_pwd_periodic_change_enabled

IMS Entry	Enable password aging?
Location	AccessAdmin > System > System policies > Password Policies > Password Aging Policies
Description	Whether to enable password aging? User must do periodic password change.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none">• #True: Yes• #False: No (default value)
Scope	System
Note	Refreshed on sync.



pid_enc_pwd_change_days

IMS Entry	Maximum password age, in days
Location	AccessAdmin > System > System policies > Password Policies > Password Aging Policies
Description	Maximum password age, in days. It is the period between two password changes for a Wallet. Note: Effective only if password periodic change is enabled.
Registry	
Type	Positive integer
Values	90 (default value)
Scope	System
Note	Refreshed on sync.

 pid_enc_pwd_expiry_reminder_enabled

IMS Entry	Enable password change reminder?
Location	AccessAdmin > System > System policies > Password Policies > Password Aging Policies
Description	Whether to remind the user about the expiring password. Note: Effective only if password periodic change is enabled.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none"> • #True: Yes • #False: No (default value)
Scope	System
Note	Refreshed on sync.

 pid_enc_pwd_expiry_reminder_days

IMS Entry	Number of days before password expiry to start reminding user
Location	AccessAdmin > System > System policies > Password Policies > Password Aging Policies
Description	Number of days before password expiry to start reminding the user. Note: This policy is effective only if password expiry reminder is enabled.
Registry	
Type	Non-negative integers
Values	5 (default value)
Scope	System
Note	<ul style="list-style-type: none"> • Value ranges from 1 to 10. • Refreshed on sync.

 pid_enc_pwd_expiry_change_enforced

IMS Entry	Enforce password change on expiry?
Location	AccessAdmin > System > System policies > Password Policies > Password Aging Policies
Description	Whether to enforce password change on expiry. The user is prompted to change the password before logon to IBM Security Access Manager for Enterprise Single Sign-On. Note: Effective only if password periodic change is enabled.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none"> • #True: Yes • #False: No (default value)
Scope	System
Note	Refreshed on sync.

Password change policies

Know the different password change policies, where to find and set these policies, their descriptions, and their default values.

pid_enc_pwd_reset_option

IMS Entry	Enable password reset?
Location	AccessAdmin > System > System policies > Password Policies > Password Change Policies
Description	Whether to enable password reset. Note: <ol style="list-style-type: none"> For option 2, the links in the ESSO GINA welcome screen and AccessAgent UI is removed if no user is logged on. The options affect AccessAgent only. AccessAssistant and Web Workplace are not affected by the policy.
Registry	
Type	Non-negative integer
Values	<ul style="list-style-type: none"> #1: Enable password reset link (default value) #2: Disable password reset link
Scope	System
Note	Refreshed on sync.

pid_enc_pwd_change_option

IMS Entry	Enable changing of password?
Location	AccessAdmin > System > System policies > Password Policies > Password Change Policies
Description	Whether to enable changing of password. Note: <ol style="list-style-type: none"> For option 2, the links in the ESSO GINA welcome screen, ESSO GINA locked screen, AccessAgent UI, and AccessAgent Tray right-click menu are removed. If the password is configured to expire, the user is prompted to change password during logon. If the Active Directory password synchronization is enabled and the Active Directory password expires, the user is prompted to change the password. If change password is forced during initial logon, the user sees the password change prompt upon initial logon. The options affect AccessAgent only. AccessAssistant and Web Workplace are not affected by the policy.
Registry	
Type	
Values	<ul style="list-style-type: none"> #1: Enable password change link (default value) #2: Disable password change link
Scope	System
Note	Refreshed on sync.


pid_enc_pwd_change_on_first_logon_enabled

IMS Entry	Force provisioned users to change the password at first logon?
Location	AccessAdmin > System > System policies > Password Policies > Password Change Policies
Description	Whether provisioned users are forced to change the ISAM ESSO Password at first logon. Note: <ol style="list-style-type: none"> 1. This policy is only effective for provisioned users and if the ISAM ESSO Passwords are synchronized with the Active Directory passwords. 2. If the ISAM ESSO Passwords are synchronized with the Active Directory passwords, the provisioned users are forced to change passwords according to the Active Directory setting for User must change password at next logon. 3. This feature is not supported for fingerprint logon.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none"> • #True: Yes (default value) • #False: No
Scope	System
Note	Refreshed on logon.


pid_inject_winlogon_password_on_change_disabled

IMS Entry	
Location	Registry Editor > HKEY_LOCAL_MACHINE > SOFTWARE > IBM > ISAM ESSO > DeploymentOptions
Description	Whether to disable the injection of the Windows login password to the Windows Change Password screen. Note: This policy is only applicable to Windows 7 and later.
Registry	[D0] "InjectWinlogonPasswordOnChangeDisabled"
Type	DWORD
Values	<ul style="list-style-type: none"> • #0: No (default value) • #1: Yes
Scope	Machine
Note	Refreshed on use.

Password strength policies

Know the different policies for strengthening the password, where to find and set these policies, their descriptions, and their default values. Password strength policies follows the Active Directory password synchronization.


pid_enc_pwd_min_length

IMS Entry	Minimum password length
Location	AccessAdmin > System > System policies > Password Policies > Password Strength Policies


pid_enc_pwd_min_length

Description	Minimum length of an acceptable password. Note: Not effective if Active Directory password synchronization is enabled. Active Directory password strength policies are used instead.
Registry	
Type	Positive integer
Values	6 (default value)
Scope	System
Note	<ul style="list-style-type: none"> • Value ranges from 1 to 99. • Refreshed on sync.


pid_enc_pwd_max_length

IMS Entry	Maximum password length
Location	AccessAdmin > System > System policies > Password Policies > Password Strength Policies
Description	Maximum length of an acceptable password. Note: Not effective if Active Directory password synchronization is enabled. Active Directory password strength policies are used instead.
Registry	
Type	Positive integer
Values	20 (default value)
Scope	System
Note	<ul style="list-style-type: none"> • Value ranges from 1 to 99. • Refreshed on sync.


pid_enc_pwd_min_numerics_length

IMS Entry	Minimum number of numeric characters
Location	AccessAdmin > System > System policies > Password Policies > Password Strength Policies
Description	Minimum number of numeric characters for an acceptable password. Note: Not effective if Active Directory password synchronization is enabled. Active Directory password strength policies are used instead.
Registry	
Type	Non-negative integer
Values	0 (default value)
Scope	System
Note	<ul style="list-style-type: none"> • Value ranges from 0 to 99. • Refreshed on sync.


pid_enc_pwd_min_alphabets_length

IMS Entry	Minimum number of alphabetic characters
------------------	---

 pid_enc_pwd_min_alphabets_length

Location	AccessAdmin > System > System policies > Password Policies > Password Strength Policies
Description	Minimum number of alphabetic characters for an acceptable password. Note: Not effective if Active Directory password synchronization is enabled. Active Directory password strength policies are used instead.
Registry	
Type	Non-negative integer
Values	0 (default value)
Scope	System
Note	<ul style="list-style-type: none"> • Value ranges from 0 to 99. • Refreshed on sync.

 pid_enc_pwd_mixed_case_enforced

IMS Entry	Enforce the use of both upper case and lower case characters?
Location	AccessAdmin > System > System policies > Password Policies > Password Strength Policies
Description	Whether to enforce the use of both upper case and lower case characters for the password. Note: Not effective if Active Directory password synchronization is enabled. Active Directory password strength policies are used instead.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none"> • #True: Yes • #False: No (default value)
Scope	System
Note	Refreshed on sync.

Chapter 6. Policies for Sign up and Password Reset

Use the sign up and password reset policies to configure the different self-service features, such as sign-up and password reset.

For more information:

- “Self-service password reset policies”
- “Self-service registration and bypass of second factor policies” on page 16
- “Sign up policies” on page 17

Self-service password reset policies

Know the different self-service password reset policies, where to find and set these policies, their descriptions, and their default values.



pid_selfhelp_password_reset_enabled

IMS Entry	Enable self-service password reset?
Location	AccessAdmin > System > System policies > Self-service Policies > Self-service Password Reset Policies
Description	Whether to enable self-service password reset.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none">• #True: Yes• #False: No (default value)
Scope	System
Note	



pid_secrets_register_for_selfhelp_max

IMS Entry	Maximum number of secret questions a user can register to enable self-service
Location	AccessAdmin > System > System policies > Self-service Policies > Self-service Password Reset Policies
Description	Maximum number of secret questions a user can register to enable self-service
Registry	
Type	Positive integer
Values	3 (default value)
Scope	System
Note	Refreshed on sync.



pid_secrets_verify_for_selfhelp

IMS Entry	The number of secret questions the user must answer to use self-service.
------------------	--

 pid_secrets_verify_for_selfhelp

Location	AccessAdmin > System > System policies > Self-service Policies > Self-service Password Reset Policies
Description	The number of secret questions the user must answer to use self-service password reset.
Registry	
Type	Positive integer
Values	2 (default value)
Scope	System
Note	Refreshed on sync.

 pid_secrets_verify_invalid_trial_count_max


IMS Entry	The maximum number of invalid login attempts allowed before self-service locks out.
Location	AccessAdmin > System > System policies > Self-service Policies > Self-service Password Reset Policies
Description	The maximum number of allowed attempts with wrong secret answers before the self-service function is locked.
Registry	
Type	Positive integer
Values	6 (default value)
Scope	System
Note	Refreshed on sync.

Self-service registration and bypass of second factor policies

Know the different self-service registration policies, where to find and set these policies, their descriptions, and their default values.

 pid_selfhelp_second_factor_registration_and_bypass_enabled

IMS Entry	Enable self-service registration and bypass of second factor?
Location	AccessAdmin > System > System policies > Self-service Policies > Self-service Registration and Bypass of Second Factor Policies
Description	Whether to enable self-service registration and bypass of a second factor. Note: <ol style="list-style-type: none"> 1. If this policy is enabled, the user can bypass the use of a second factor for logon by providing registered secrets. 2. If an authorization code is required for the second-factor registration, the user can do a self-service registration by providing registered secrets. 3. If the user cannot provide registered secrets, there is an option to provide an authorization code and the primary secret.
Registry	
Type	Boolean

 pid_selfhelp_second_factor_registration_and_bypass_enabled

Values	<ul style="list-style-type: none"> • #True: Yes • #False: No (default value)
Scope	System
Note	Refreshed on sync.

Sign up policies

Know the different sign up policies, where to find and set these policies, their descriptions, and their default values.

 pid_second_factor_for_sign_up_required


IMS Entry	Require authentication second factor during sign up?
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > Sign Up Policies
Description	<p>Whether a second factor is required during sign up.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. Enable this policy if a second factor is required during sign up. Second authentication factors that are defined in the user policy template can be implemented only after user registration. 2. Effective only if the second factors supported list is not empty. In this case, any one of the supported second factors can be used for sign up. There is one UI dialog that requests the user to present any one of the supported second factors. 3. If policy value is 1, sign up fails if the second factor is not presented.
Registry	[D0] "SecondFactorForSignUpRequired"
Type	DWORD
Values	<ul style="list-style-type: none"> • #True: Yes • #False: No (default value)
Scope	Machine
Note	Refreshed on use.

 pid_automatic_sign_up_enabled

IMS Entry	Enable automatic sign up?
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > Sign Up Policies
Description	<p>Whether to enable automatic sign up.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. This policy must be set to 1 if password is synchronized with Active Directory password. 2. pid_engina_welcome_text and pid_unlock_text must be modified if this policy is set to 1. 3. If this policy is set to 1, the Sign up option is not available on both the AccessAgent UI and AccessAgent Tray menu. The user is not prompted to sign up if the user logs on to an unregistered user name. The user is not prompted to confirm sign up if an unregistered second factor is presented.


pid_automatic_sign_up_enabled

Registry	[D0] "AutomaticSignUpEnabled"
Type	DWORD
Values	<ul style="list-style-type: none"> • #True: Yes • #False: No (default value)
Scope	Machine
Note	Refreshed on use.


pid_bind_secret_question_list

IMS Entry	Question set for secret
Location	AccessAdmin > System > System policies > Sign Up Policies
Description	<p>The set of questions user can choose from during sign-up to provide the secret answer.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. The system cannot display the entire secret question if it is longer than the screen width. 2. This message is available in multiple languages. It is displayed in the language that is specified by the user during an AccessAgent installation.
Registry	
Type	String list
Values	<ul style="list-style-type: none"> • Whats your favorite color? • Whats your favorite fruit? • Whats your mother's maiden name? • Who's your favorite author? • Who's your favorite composer? • Who's your favorite person from history?
Scope	System
Note	<ul style="list-style-type: none"> • You can select multiple values. • Refreshed on sync.


pid_secret_answer_min_length

IMS Entry	Minimum length of an acceptable secret answer
Location	AccessAdmin > System > System policies > Sign Up Policies
Description	Minimum length of an acceptable secret answer.
Registry	
Type	Positive integer
Values	3 (default value)
Scope	System
Note	Refreshed on sync.



pid_secrets_register_for_selfhelp_at_sign_up

IMS Entry	Prompt user to register additional secrets for self-service during sign up?
Location	AccessAdmin > System > System policies > Sign Up Policies
Description	Whether to prompt the user to register additional secrets for self-service during sign up. Note: If pid_secrets_verify_for_selfhelp is 1, the user is not prompted to register more secrets, because the primary secret is sufficient for the self-service actions. The user can still choose to register more secrets after logon by clicking Set self-service secrets in AccessAgent.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none"> • #True: Yes • #False: No (default value)
Scope	System
Note	Refreshed on sync.



pid_secret_option

IMS Entry	Option for specifying secret
Location	AccessAdmin > System > System policies > Sign Up Policies
Description	Whether the secret is required, it must be specified by the user during sign up. Note: <ol style="list-style-type: none"> 1. This policy applies to users who are signing up or who are logging on for the first time after their accounts have been pre-provisioned. 2. For policy value 0, the user is assigned a system-defined secret. The user is not prompted for a secret when performing actions that require it (for example, reset password and offline recovery). The customer must understand the security implications to using a system-defined secret before the implementation of such a configuration. 3. If the policy value is changed from 1 to 0, the user is automatically migrated to a system-defined secret when the user logs on to AccessAgent successfully. 4. Once the policy value is set to 0 during sign-up, adding a user-defined primary secret later is not supported. You can only add user-defined primary secret during sign-up.
Registry	
Type	Non-negative integer
Values	<ul style="list-style-type: none"> • #0: Secret not required. • #1: Secret required, and user must specify during sign up. (default)
Scope	System
Note	Refreshed on sync.

Chapter 7. Policies for Configurable Text and Accessibility

This section provides all the policies that you must configure for configurable text and accessibility features. The values in the configurable text policies are stored in multiple languages, depending on the language that is specified by the user during an AccessAgent installation.

For more information:

- “Configurable text policies”
- “Accessibility policy” on page 35

Configurable text policies

View the details of the different configurable text policies. To enter text policies for multiple languages, the Administrator must log on to AccessAdmin multiple times and select a different language each time.

For more information:

- “ESSO GINA text policies”
- “Unlock text policies” on page 25
- “Sign up text policies” on page 34
- “AccessAssistant and Web Workplace text policies” on page 35

ESSO GINA text policies

Know the different configurable text policies for ESSO GINA or Credential Provider, where to find and set these policies, their descriptions, and their default values.



pid_engina_welcome_text

IMS Entry	Welcome message (Maximum 2 lines)
Location	AccessAdmin > System > System policies > Configurable Text Policies > ESSO GINA Text Policies
Description	Configurable text for the ESSO GINA welcome message. Note: <ol style="list-style-type: none">1. This message is displayed, followed by a blank line, and then the messages in one of the listed configurable text policies (depending on the list of supported second factors).2. The two lines of messages are separated by a blank line.3. “\n\n” can be added if more blank lines are necessary.4. This message is available in multiple languages. It is displayed in the language that is specified by the user during an AccessAgent installation.
Registry	
Type	String list
Values	This computer is protected by ISAM ESSO AccessAgent. If you are here for the first time, click 'Sign up' to get started.
Scope	System


pid_engina_welcome_text

Note	<ul style="list-style-type: none"> • Maximum of 2 strings. • Each text box can contain about 40 characters per line, and contain a maximum of 15 lines. • Refreshed on sync.
-------------	---


pid_logon_credentials_text

IMS Entry	Logon credentials message (Maximum 1 line)
Location	AccessAdmin > System > System policies > Configurable Text Policies > ESSO GINA Text Policies
Description	<p>Configurable text that is to be displayed right above the logon credentials when the user clicks Log on.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. If pid_enc_pwd_is_ad_pwd_enabled is set to True, this policy must be modified, for example, Enter your Windows domain user name and password to log on. 2. This message is available in multiple languages. It is displayed in the language that is specified by the user during an AccessAgent installation.
Registry	
Type	String list
Values	Enter your user name and password to log on.
Scope	System
Note	<ul style="list-style-type: none"> • Maximum of 1 string. • Text box takes 2 lines max, about 40 characters per line. • Refreshed on sync.


pid_engina_logon_with_pwd_text

IMS Entry	Instructions for password logon (Maximum 2 lines)
Location	AccessAdmin > System > System policies > Configurable Text Policies > ESSO GINA Text Policies
Description	<p>Configurable text for password logon.</p> <p>Note: See pid_engina_welcome_text.</p>
Registry	
Type	String list
Values	To log on, click 'Log on'.
Scope	System
Note	<ul style="list-style-type: none"> • Maximum of 2 strings. • Each text box can contain about 40 characters per line, and contain a maximum of 15 lines. • Refreshed on sync.



pid_engina_logon_with_rfid_text

IMS Entry	Instructions for RFID logon (Maximum 2 lines)
Location	AccessAdmin > System > System policies > Configurable Text Policies > ESSO GINA Text Policies
Description	Configurable text for RFID logon. Note: See pid_engina_welcome_text.
Registry	
Type	String list
Values	To log on, tap your RFID card. If you do not have your RFID card, click 'Log on'.
Scope	System
Note	<ul style="list-style-type: none"> • Maximum of 2 strings. • Each text box can contain about 40 characters per line, and contain a maximum of 15 lines. • Refreshed on sync.



pid_engina_logon_with_sc_text

IMS Entry	Instructions for smart card logon (Maximum 2 lines)
Location	AccessAdmin > System > System policies > Configurable Text Policies > ESSO GINA Text Policies
Description	Configurable text for smart card logon. Note: See pid_engina_welcome_text.
Registry	
Type	String list
Values	To log on, insert your smart card. If you have already inserted your smart card and you are not prompted for a PIN, remove and reinsert your smart card. If you do not have your smart card, click 'Log on'.
Scope	System
Note	<ul style="list-style-type: none"> • Maximum of 2 strings. • Each text box can contain about 40 characters per line, and contain a maximum of 15 lines. • Refreshed on sync.



pid_engina_logon_with_hsc_text

IMS Entry	Instructions for hybrid smart card logon (Maximum 2 lines)
Location	AccessAdmin > System > System policies > Configurable Text Policies > ESSO GINA Text Policies
Description	Configurable text for hybrid smart card logon.
Registry	
Type	String list


pid_engina_logon_with_hsc_text

Values	To log on, tap your hybrid smart card. If you do not have your hybrid smart card, click 'Log on'.
Scope	System
Note	<ul style="list-style-type: none"> • Maximum of 2 strings. • Each text box can contain about 40 characters per line, and contain a maximum of 15 lines. • Refreshed on sync.


pid_engina_logon_with_fingerprint_text

IMS Entry	Instructions for fingerprint logon (Maximum 2 lines)
Location	AccessAdmin > System > System policies > Configurable Text Policies > ESSO GINA Text Policies
Description	Configurable text for fingerprint logon. Note: See pid_engina_welcome_text.
Registry	
Type	String list
Values	To log on, place your registered finger on the sensor. To log on without fingerprint, click 'Log on'.
Scope	System
Note	<ul style="list-style-type: none"> • Maximum of 2 strings. • Each text box can contain about 40 characters per line, and contain a maximum of 15 lines. • Refreshed on sync.


pid_engina_bypass_automatic_text

IMS Entry	Message for automatic ESSO GINA bypass
Location	AccessAdmin > System > System policies > Configurable Text Policies > ESSO GINA Text Policies
Description	Configurable text message for automatic ESSO GINA bypass. Note: This message is available in multiple languages. It is displayed in the language that is specified by the user during an AccessAgent installation.
Registry	
Type	String
Values	AccessAgent is currently unable to connect to the IMS Server to log on to your Wallet. You may proceed to log on to Windows but single sign-on is disabled.
Scope	System
Note	Refreshed on sync.



pid_engina_logon_with_fingerprint_or_rfid_text

IMS Entry	Instructions for fingerprint or RFID logon (Maximum 2 lines)
Location	AccessAdmin > System > System policies > Configurable Text Policies > ESSO GINA Text Policies
Description	Configurable text for fingerprint or RFID logon. Note: See pid_engina_welcome_text.
Registry	
Type	String list
Values	To log on, place your registered finger on the sensor or tap your RFID card. To log on without fingerprint or RFID card, click 'Log on'.
Scope	System
Note	<ul style="list-style-type: none"> • Maximum of 2 strings. • Each text box can contain about 40 characters per line, and contain a maximum of 15 lines. • Refreshed on sync.

Unlock text policies

Know the different unlock configurable text policies, where to find and set these policies, their descriptions, and their default values.



pid_unlock_text

IMS Entry	Locked computer message (Maximum 1 line)
Location	AccessAdmin > System > System policies > Configurable Text Policies > Unlock Text Policies
Description	Configurable text for a computer locked message. Note: <ol style="list-style-type: none"> 1. This message is displayed, followed by a blank line, and then messages in one of the configurable unlock text policies (depending on current Wallet and pid_unlock_option). 2. The two lines of messages are separated by a blank line. 3. "\n\n" can be added if more blank lines are necessary. 4. This message is available in multiple languages. It is displayed in the language that is specified by the user during an AccessAgent installation.
Registry	
Type	String list
Values	This computer is protected by ISAM ESSO AccessAgent, and has been locked.
Scope	System
Note	<ul style="list-style-type: none"> • Maximum of 1 string. • Each text box can contain about 40 characters per line, and contain a maximum of 15 lines. • Refreshed on sync.


pid_unlock_credentials_text

IMS Entry	Unlock credentials message (Maximum 1 line)
Location	AccessAdmin > System > System policies > Configurable Text Policies > Unlock Text Policies
Description	Configurable text that is to be displayed right above the unlock credentials when the user clicks Unlock this computer . Note: <ol style="list-style-type: none"> 1. If Active Directory password synchronization is enabled, this policy must be modified. For example, Enter your Windows domain user name and password to unlock. 2. This message is available in multiple languages. It is displayed in the language that is specified by the user during an AccessAgent installation.
Registry	
Type	String list
Values	Enter your user name and password to unlock.
Scope	System
Note	<ul style="list-style-type: none"> • Maximum of 1 string. • Each text box can contain about 40 characters per line, and contain a maximum of 15 lines. • Refreshed on sync.


pid_unlock_with_pwd_option_1_text

IMS Entry	Instructions for unlocking with password when unlock policy is 'only the same user can unlock' (Maximum 2 lines)
Location	AccessAdmin > System > System policies > Configurable Text Policies > Unlock Text Policies
Description	Configurable text for unlocking with a password when the computer is locked and pid_unlock_option is 1. Note: See pid_unlock_text.
Registry	
Type	String list
Values	To unlock, click 'Unlock this computer'.
Scope	System
Note	<ul style="list-style-type: none"> • Maximum of 2 strings. • Each text box can contain about 40 characters per line, and contain a maximum of 15 lines. • Refreshed on sync.


pid_unlock_with_pwd_option_3_text

IMS Entry	Instructions for unlocking with password when unlock policy is 'any user with or without current desktop account in Wallet can unlock' (Maximum 2 lines)
Location	AccessAdmin > System > System policies > Configurable Text Policies > Unlock Text Policies



pid_unlock_with_pwd_option_3_text

Description	Configurable text for unlocking with a password when the computer is locked and pid_unlock_option is 3. Note: See pid_unlock_text.
Registry	
Type	String list
Values	To unlock, click 'Unlock this computer'.
Scope	System
Note	<ul style="list-style-type: none"> • Maximum of 2 strings. • Each text box can contain about 40 characters per line, and contain a maximum of 15 lines. • Refreshed on sync.



pid_unlock_with_pwd_option_4_text

IMS Entry	Instructions for unlocking with password when unlock policy is 'only the same user can unlock, but different user can re-log on to Windows' (Maximum 2 lines)
Location	AccessAdmin > System > System policies > Configurable Text Policies > Unlock Text Policies
Description	Configurable text for unlocking with a password when the computer is locked and pid_unlock_option is 4. Note: See pid_unlock_text.
Registry	
Type	String list
Values	To unlock, click 'Unlock this computer'.
Scope	System
Note	<ul style="list-style-type: none"> • Maximum of 2 strings. • Each text box can contain about 40 characters per line, and contain a maximum of 15 lines. • Refreshed on sync.



pid_unlock_with_sc_option_1_text

IMS Entry	Instructions for unlocking with smart card when unlock policy is 'only the same user can unlock' (Maximum 2 lines)
Location	AccessAdmin > System > System policies > Configurable Text Policies > Unlock Text Policies
Description	Configurable text for unlocking with a smart card when the computer is locked and pid_unlock_option is 1. Note: See pid_unlock_text.
Registry	
Type	String list


pid_unlock_with_sc_option_1_text

Values	To unlock, insert your smart card. If you have already inserted your smart card and you are not prompted for a PIN, remove and reinsert your smart card. If you do not have your smart card, click 'Unlock this computer'.
Scope	System
Note	<ul style="list-style-type: none"> • Maximum of 2 strings. • Each text box can contain about 40 characters per line, and contain a maximum of 15 lines. • Refreshed on sync.


pid_unlock_with_sc_option_3_text

IMS Entry	Instructions for unlocking with smart card when unlock policy is 'any user with or without current desktop account in Wallet can unlock' (Maximum 2 lines)
Location	AccessAdmin > System > System policies > Configurable Text Policies > Unlock Text Policies
Description	Configurable text for unlocking with a smart card when the computer is locked and pid_unlock_option is 3. Note: See pid_unlock_text.
Registry	
Type	String list
Values	To unlock, insert your smart card. If you have already inserted your smart card and you are not prompted for a PIN, remove and reinsert your smart card. If you do not have your smart card, click 'Unlock this computer'.
Scope	System
Note	<ul style="list-style-type: none"> • Maximum of 2 strings. • Each text box can contain about 40 characters per line, and contain a maximum of 15 lines. • Refreshed on sync.


pid_unlock_with_sc_option_4_text

IMS Entry	Instructions for unlocking with smart card when unlock policy is 'only the same user can unlock, but different user can re-log on to Windows' (Maximum 2 lines)
Location	AccessAdmin > System > System policies > Configurable Text Policies > Unlock Text Policies
Description	Configurable text for unlocking with a smart card when the computer is locked and pid_unlock option is 4. Note: See pid_unlock_text.
Registry	
Type	String list



pid_unlock_with_sc_option_4_text

Values	To unlock, insert your smart card. If you have already inserted your smart card and you are not prompted for a PIN, remove and reinsert your smart card. If you do not have your smart card, click 'Unlock this computer'.
Scope	System
Note	<ul style="list-style-type: none"> • Maximum of 2 strings. • Each text box can contain about 40 characters per line, and contain a maximum of 15 lines. • Refreshed on sync.



pid_unlock_with_hsc_option_1_text

IMS Entry	Instructions for unlocking with hybrid smart card when unlock policy is 'only the same user can unlock' (Maximum 2 lines)
Location	AccessAdmin > System > System policies > Configurable Text Policies > Unlock Text Policies
Description	Configurable text for unlocking with a hybrid smart card when the computer is locked and pid_unlock_option is 1. Note: See pid_unlock_text.
Registry	
Type	String list
Values	To unlock, tap your hybrid smart card. If you do not have your hybrid smart card, click 'Unlock this computer'.
Scope	System
Note	<ul style="list-style-type: none"> • Maximum of 2 strings. • Each text box can contain about 40 characters per line, and contain a maximum of 15 lines. • Refreshed on sync.



pid_unlock_with_hsc_option_3_text

IMS Entry	Instructions for unlocking with hybrid smart card when the unlock policy is 'any user with or without current desktop account in Wallet can unlock' (Maximum 2 lines)
Location	AccessAdmin > System > System policies > Configurable Text Policies > Unlock Text Policies
Description	Configurable text for unlocking with a hybrid smart card when the computer is locked and pid_unlock_option is 3. Note: See pid_unlock_text.
Registry	
Type	String list
Values	To unlock, tap your hybrid smart card. If you do not have your hybrid smart card, click 'Unlock this computer'.
Scope	System


pid_unlock_with_hsc_option_3_text

Note	<ul style="list-style-type: none"> • Maximum of 2 strings. • Each text box can contain about 40 characters per line, and contain a maximum of 15 lines. • Refreshed on sync.
-------------	---


pid_unlock_with_hsc_option_4_text

IMS Entry	Instructions for unlocking with hybrid smart card when unlock policy is 'only the same user can unlock, but different user can re-log on to Windows' (Maximum 2 lines)
Location	AccessAdmin > System > System policies > Configurable Text Policies > Unlock Text Policies
Description	Configurable text for unlocking with a hybrid smart card when the computer is locked and pid_unlock option is 4. Note: See pid_unlock_text.
Registry	
Type	String list
Values	To unlock, tap your hybrid smart card. If you do not have your hybrid smart card, click 'Unlock this computer'.
Scope	System
Note	<ul style="list-style-type: none"> • Maximum of 2 strings. • Each text box can contain about 40 characters per line, and contain a maximum of 15 lines. • Refreshed on sync.


pid_unlock_with_rfid_option_1_text

IMS Entry	Instructions for unlocking with RFID when unlock policy is 'only the same user can unlock' (Maximum 2 lines)
Location	AccessAdmin > System > System policies > Configurable Text Policies > Unlock Text Policies
Description	Configurable text for unlocking with an RFID when the computer is locked and pid_unlock_option is 1. Note: See pid_unlock_text.
Registry	
Type	String list
Values	To unlock, tap your RFID card. If you do not have your RFID card, click 'Unlock this computer'.
Scope	System
Note	<ul style="list-style-type: none"> • Maximum of 2 strings. • Each text box can contain about 40 characters per line, and contain a maximum of 15 lines. • Refreshed on sync.



pid_unlock_with_rfid_option_3_text

IMS Entry	Instructions for unlocking with RFID when unlock policy is 'any user with or without current desktop account in Wallet can unlock' (Maximum 2 lines)
Location	AccessAdmin > System > System policies > Configurable Text Policies > Unlock Text Policies
Description	Configurable text for unlocking with an RFID when the computer is locked and pid_unlock_option is 3. Note: See pid_unlock_text.
Registry	
Type	String list
Values	To unlock, tap your RFID card. If you do not have your RFID card, click 'Unlock this computer'.
Scope	System
Note	<ul style="list-style-type: none"> • Each text box can contain about 40 characters per line, and contain a maximum of 15 lines. • Refreshed on sync.



pid_unlock_with_rfid_option_4_text

IMS Entry	Instructions for unlocking with RFID when unlock policy is 'only the same user can unlock, but different user can re-log on to Windows' (Maximum 2 lines)
Location	AccessAdmin > System > System policies > Configurable Text Policies > Unlock Text Policies
Description	Configurable text for unlocking with an RFID when the computer locked and pid_unlock_option is 4. Note: See pid_unlock_text.
Registry	
Type	String list
Values	To unlock, tap your RFID card. If you do not have your RFID card, click 'Unlock this computer'.
Scope	System
Note	<ul style="list-style-type: none"> • Each text box can contain about 40 characters per line, and contain a maximum of 15 lines. • Refreshed on sync.



pid_unlock_with_fingerprint_option_1_text

IMS Entry	Instructions for unlocking with fingerprint when unlock policy is 'only the same user can unlock' (Maximum 2 lines)
Location	AccessAdmin > System > System policies > Configurable Text Policies > Unlock Text Policies
Description	Configurable text for unlocking with a fingerprint when the computer is locked and pid_unlock_option is 1. Note: See pid_unlock_text.


pid_unlock_with_fingerprint_option_1_text

Registry	
Type	String list
Values	To unlock, place your registered finger on the sensor. To unlock without fingerprint, click 'Unlock this computer'.
Scope	System
Note	<ul style="list-style-type: none"> • Maximum of 2 strings. • Each text box can contain about 40 characters per line, and contain a maximum of 15 lines. • Refreshed on sync.


pid_unlock_with_fingerprint_option_3_text

IMS Entry	Instructions for unlocking with fingerprint when unlock policy is 'any user with or without current desktop account in Wallet can unlock' (Maximum 2 lines)
Location	AccessAdmin > System > System policies > Configurable Text Policies > Unlock Text Policies
Description	Configurable text for unlocking with a fingerprint when the computer is locked and pid_unlock_option is 3. Note: See pid_unlock_text.
Registry	
Type	String list
Values	To unlock, place your registered finger on the sensor. To unlock without fingerprint, click 'Unlock this computer'.
Scope	System
Note	<ul style="list-style-type: none"> • Maximum of 2 strings. • Each text box can contain about 40 characters per line, and contain a maximum of 15 lines. • Refreshed on sync.


pid_unlock_with_fingerprint_option_4_text

IMS Entry	Instructions for unlocking with fingerprint when unlock policy is 'only the same user can unlock, but different user can re-log on to Windows' (Maximum 2 lines)
Location	AccessAdmin > System > System policies > Configurable Text Policies > Unlock Text Policies
Description	Configurable text for unlocking with a fingerprint when the computer is locked and pid_unlock_option is 4. Note: See pid_unlock_text.
Registry	
Type	String list
Values	To unlock, place your registered finger on the sensor. To unlock without fingerprint, click 'Unlock this computer'.



pid_unlock_with_fingerprint_option_4_text

Scope	System
Note	<ul style="list-style-type: none"> • Maximum of 2 strings. • Each text box can contain about 40 characters per line, and contain a maximum of 15 lines. • Refreshed on sync.



pid_unlock_with_fingerprint_or_rfid_option_1_text

IMS Entry	Instructions for unlocking with fingerprint or RFID when unlock policy is 'only the same user can unlock' (Maximum 2 lines)
Location	AccessAdmin > System > System policies > Configurable Text Policies > Unlock Text Policies
Description	Configurable text for unlocking with a fingerprint or an RFID when the computer is locked and pid_unlock_option is 1. Note: See pid_unlock_text.
Registry	
Type	String list
Values	To unlock, place your registered finger on the sensor or tap your RFID card. To unlock without fingerprint or RFID card, click 'Unlock this computer'.
Scope	System
Note	<ul style="list-style-type: none"> • Maximum of 2 strings. • Each text box can contain about 40 characters per line, and contain a maximum of 15 lines. • Refreshed on sync.



pid_unlock_with_fingerprint_or_rfid_option_3_text

IMS Entry	Instructions for unlocking with fingerprint or RFID when unlock policy is 'any user with or without current desktop account in Wallet can unlock' (Maximum 2 lines)
Location	AccessAdmin > System > System policies > Configurable Text Policies > Unlock Text Policies
Description	Configurable text for unlocking with a fingerprint or an RFID when the computer is locked and pid_unlock_option is 3. Note: See pid_unlock_text.
Registry	
Type	String list
Values	To unlock, place your registered finger on the sensor or tap your RFID card. To unlock without fingerprint or RFID card, click 'Unlock this computer'.
Scope	System
Note	<ul style="list-style-type: none"> • Maximum of 2 strings. • Each text box can contain about 40 characters per line, and contain a maximum of 15 lines. • Refreshed on sync.


pid_unlock_with_fingerprint_or_rfid_option_4_text

IMS Entry	Instructions for unlocking with fingerprint or RFID when unlock policy is 'only the same user can unlock, but different user can relog on to Windows' (Maximum 2 lines)
Location	AccessAdmin > System > System policies > Configurable Text Policies > Unlock Text Policies
Description	Configurable text for unlocking with a fingerprint or an RFID when the computer is locked and pid_unlock option is 4. Note: See pid_unlock_text.
Registry	
Type	String list
Values	To unlock, place your registered finger on the sensor or tap your RFID card. To unlock without fingerprint or RFID card, click 'Unlock this computer'.
Scope	System
Note	<ul style="list-style-type: none"> • Maximum of 2 strings. • Each text box can contain about 40 characters per line, and contain a maximum of 15 lines. • Refreshed on sync.

Sign up text policies

Know the different sign up configurable text policies, where to find and set these policies, their descriptions, and their default values.


pid_bind_display_template

IMS Entry	Template for sign-up dialog
Location	AccessAdmin > System > System policies > Configurable Text Policies > Sign Up Text Policies
Description	The template to be used for displaying the sign-up dialog. Note: <ol style="list-style-type: none"> 1. The Domain field is shown if the enterprise directory is the Active Directory. 2. Other than the domain, the template can support either one or two fields only. To display only one field, set the Label of one of the fields to a blank entry. The field with the blank Label is not displayed.
Registry	
Type	Bind template
Values	Enter your domain user name and password for identity verification. User name Password
Scope	System
Note	Refreshed on sync.

AccessAssistant and Web Workplace text policies

Know the different configurable text policies for AccessAssistant and Web Workplace, where to find and set these policies, their descriptions, and their default values.



pid_accessanywhere_otp_reset_link_text

IMS Entry	Text for the OTP (OATH) reset link on AccessAssistant and Web Workplace.
Location	AccessAdmin > System > System policies > Configurable Text Policies > AccessAssistant and Web Workplace Text Policies
Description	Configurable text for the OTP (OATH) reset link on AccessAssistant and Web Workplace. Note: Effective only if pid_auth_authentication_option for AccessAnywhere contains OTP (OATH).
Registry	
Type	String
Values	Reset OTP token
Scope	System
Note	Refreshed on sync.

Accessibility policy

Know the policy to enable accessibility features, and where to find and set this policy.



pid_accessibility_is_animation_enabled

IMS Entry	Enable animation?
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Accessibility Policies
Description	Whether to enable or not enable the accessibility features for visually impaired users, including animation effect and jaws-readable screen.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none">• #False: No• #True: Yes (default value)
Scope	Machine
Note	

Chapter 8. Policies for Private and Shared desktops

Use private and shared desktop policies to configure settings for private and shared desktop deployments.

In a shared desktop mode, multiple users share a generic Windows desktop in one workstation. In a private desktop mode, users have their own Windows desktops in a workstation.

For more information:

- “Shared workstation policies”

Shared workstation policies

Know the different policies for a shared workstation, where to find and set these policies, their descriptions, and their default values. All pid_lusm_ policies are only applicable to Windows XP.

Lock/Unlock Policies

pid_win_startup_action

IMS Entry	Windows startup actions
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > Shared Workstation Policies > Lock/Unlock Policies
Description	Actions on Windows startup. Note: Use this policy to enable automatic locking of the computer after AutoAdminLogon or ForceAutoLogon .
Registry	[D0] "WinStartupAction"
Type	DWORD
Values	<ul style="list-style-type: none">• #0: No action (default value)• #1: Lock computer
Scope	Machine
Note	Refreshed on use.

pid_win_fast_user_switching_enabled

IMS Entry	Enable support for Windows Fast User Switching?
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > Shared Workstation Policies > Lock/Unlock Policies
Description	Whether to enable support for Fast User Switching in Microsoft Windows 7 and later versions. Note: Effective only if the client operating system is Microsoft Windows 7 and later versions, and if Fast User Switching is enabled.
Registry	[D0] "WinFastUserSwitchingEnabled"
Type	Boolean


 **pid_win_fast_user_switching_enabled**

Values	<ul style="list-style-type: none"> • #True: Yes • #False: No (default value)
Scope	Machine
Note	<ul style="list-style-type: none"> • Refreshed on sync. • For Microsoft Windows 7 and Windows 8 only. • If set to No, the environment is similar to a personal desktop with one user. • If set to Yes, there are multiple sessions in the same desktop. This behavior is similar to that of a private desktop for Windows XP.

Private Desktop Polices (Windows XP only)

 **pid_lusm_sessions_max**

IMS Entry	Maximum number of concurrent user sessions on a workstation (only for Windows XP)
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > Shared Workstation Policies > Private Desktop Policies
Description	<p>Maximum number of concurrent user sessions. Set it to 2 or a higher value to enable private desktop.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. Set policy value to 1 to not enable Local User Session Management. 2. To enable Local User Session Management, specify a value greater than 1 for this policy in the <code>DeploymentOptions.reg</code> file during an AccessAgent installation. <p>If the policy value is greater than 1 after AccessAgent is installed, the Log Off and Shut Down buttons, and Windows hot keys might be enabled for the first user who logs on.</p> <p>The buttons and Windows hot keys might also remain not enabled after AccessAgent is uninstalled.</p> <ol style="list-style-type: none"> 3. This policy can be set to a value higher than what the system resources can support. However, the actual number of concurrent user sessions is still capped by the system resources available. 4. For optimal performance, set to the value to 9 or a lower value. 5. If Local User Session Management is enabled, set <code>pid_logoff_manual_action</code> to 1 (Log off Windows). Manually logging off AccessAgent is equivalent to logging off the desktop session of the user. 6. Set <code>pid_unlock_with_win_option</code> to 0 as unlocking with Windows is not supported for Local User Session Management. <p>Enable auto-admin logon to Windows. Set <code>pid_microsoft_auto_logon_enabled</code> to 1, <code>pid_microsoft_auto_logon_acct</code> to a local computer logon account, and <code>pid_win_startup_action</code> to 1, to lock the computer immediately after logon.</p> <ol style="list-style-type: none"> 7. Modifying this policy requires a computer restart to implement the changes.
Registry	[D0] "LUSMSessionsMax"
Type	DWORD
Values	1 (default value)

 **pid_lusm_sessions_max**


Scope	Machine
Note	<ul style="list-style-type: none"> • Value range from 1 to 12. • Refreshed on startup.

 **pid_lusm_session_replacement_option**

IMS Entry	Session replacement option (only for Windows XP)
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > Shared Workstation Policies > Private Desktop Policies
Description	<p>Option for replacing existing user sessions. This option is intended for the scenario where a new user attempts to log on while the number of concurrent user sessions reached the maximum allowed number of sessions.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. Effective only if pid_lusm_sessions_max is greater than 1. 2. For policy value 2, this is useful for machines which are used by users in a sequence. 3. For policy value 3, the session that is unlocked the least number of times is replaced. 4. For policy value 4, the session that is least used in terms of total duration is replaced. 5. Computation of time for all cases is accurate only to the nearest minute. 6. Modifying this policy requires a computer restart to implement the changes.
Registry	[D0] "LUSMSessionReplacementOption"
Type	DWORD
Values	<ul style="list-style-type: none"> • #0: Disallow new user to log on • #1: Replace least recently used (LRU) session (default value) • #2: Replace most recently used (MRU) session • #3: Replace least frequently used (LFU) session • #4: Replace least used (LU) session
Scope	Machine
Note	<ul style="list-style-type: none"> • Refreshed on startup for the value Disallow new user to log on. • Refreshed on use for other values.

 **pid_lusm_sia_list**

IMS Entry	Single instance applications list (only for Windows XP)
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > Shared Workstation Policies > Private Desktop Policies


pid_lusm_sia_list

Description	<p>List of single instance applications (SIA), such as applications that cannot run multiple simultaneous instances in a computer.</p> <p>Note:</p> <ol style="list-style-type: none"> Effective only if pid_lusm_sessions_max is greater than 1. When a user starts any application in this list, AccessAgent completes the action that is specified by <ul style="list-style-type: none"> pid_lusm_sia_launch_option (if the policy value is not 0), or the launch option of the application. <p>These actions are only applicable when the application is launched from a visible desktop and there is another instance of it running in an invisible desktop. If the other instance is running in the same visible desktop, the application assumes its normal behavior.</p> For each application, the full path must be the full image path of the executable file on the disk, ending with .EXE, .BAT, or .COM. It is not case sensitive. The long path format must be used. For example, for Company Messenger, use C:\Program Files\Company\Messenger\CompanyMessenger.exe instead of C:\progra~1\Company\messenger\COMPANYM~1.exe. Modifying this policy requires a computer restart to implement the changes.
Registry	[D0] "LUSMSiaList"
Type	MULTI_SZ
Values	<p>Each application occupies three lines as follows:</p> <ul style="list-style-type: none"> Line 1: Full path of the executable file (for example, C:\Windows\notepad.exe) Line 2: Launch option. Specify any of the following numeric values: <ul style="list-style-type: none"> #1: Disallow second instance to start #2: Log off existing instance #3: Close existing instance #4: Prompt user whether to log off existing instance #5: Prompt user whether to close existing instance #6: Prompt user to forcefully close existing instance Line 3: Display name of the application (for example, Notepad)
Scope	Machine
Note	<ul style="list-style-type: none"> Empty lines are discarded. Each application must contain three lines with data or content. Refreshed on startup.


pid_lusm_sia_launch_option

IMS Entry	Action on launching a second instance of a single instance application (only for Windows XP)
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > Shared Workstation Policies > Private Desktop Policies

 **pid_lusm_sia_launch_option**

Description	Action that is taken by AccessAgent when a user launches a second instance of a single instance application. A single instance application is an application that cannot run multiple simultaneous instances on a computer. Note: <ol style="list-style-type: none"> 1. Effective only if pid_lusm_sessions_max is greater than 1. 2. If the policy value is 0, the launch option of each application (specified in pid_lusm_sia_list) is used. 3. These actions are only applicable when the application is launched from a visible desktop and there is another instance of it running in an invisible desktop. If the other instance is running in the same visible desktop, the application assumes its normal behavior. 4. Modifying this policy requires a computer restart to implement the changes.
Registry	[D0] "LUSMSiaLaunchOption"
Type	DWORD
Values	<ul style="list-style-type: none"> • #0: Use launch option of the application • #1: Disallow second instance to start • #2: Log off existing instance (default value) • #3: Close existing instance • #4: Prompt user whether to log off existing instance • #5: Prompt user whether to close existing instance • #6: Prompt user whether to forcefully close existing instance
Scope	Machine
Note	Refreshed on startup.

 **pid_lusm_generic_accounts_enabled**

IMS Entry	Enable use of generic accounts to create user desktops? (only for Windows XP)
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > Shared Workstation Policies > Private Desktop Policies
Description	Whether to use a pool of generic accounts to create user desktops. Note: <ol style="list-style-type: none"> 1. Effective only if pid_lusm_sessions_max is greater than 1. 2. If enabled, generic accounts specified in pid_lusm_generic_accounts_list create user desktops. This configuration is for deployments where some users might not exist in Active Directory, or passwords are not synchronized with the Active Directory passwords. 3. If enabled, set pid_lusm_default_desktop_preserved_enabled to 1. Important: pid_lusm_default_desktop_preserved_enabled is deprecated in the IBM Security Access Manager for Enterprise Single Sign-On v8.1 Release. For this reason, this policy does not have an IMS entry. 4. Modifying this policy requires a computer restart to implement the changes.
Registry	[D0] "LUSMGenericAccountsEnabled"
Type	DWORD

 **pid_lusm_generic_accounts_enabled**

Values	<ul style="list-style-type: none"> • #True: Yes • #False: No (default value)
Scope	Machine
Note	Refreshed on startup.

 **pid_lusm_auto_logon_acct_display_enabled**

IMS Entry	Enable display of auto-admin logon account in the logon user interface? (only for Windows XP)
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > Shared Workstation Policies > Private Desktop Policies
Description	Whether the auto-admin logon account is in the list of users that are displayed in the logon user interface of private desktops. Note: If enabled, the auto-admin logon account is displayed in the logon user interface of private desktops. Desktop administrators can click the auto-admin logon account and provide the account password for desktop maintenance when necessary.
Registry	[D0] "LUSMAutoLogonAcctDisplayEnabled"
Type	Boolean DWORD
Values	<ul style="list-style-type: none"> • #True: Yes (default value) • #False: No
Scope	Machine
Note	Refreshed on startup.

Chapter 9. Policies for Citrix and Terminal Server

Use Citrix and Terminal Server policies to manage settings for a Citrix and Terminal Server deployment.

For more information about configuring Citrix and Terminal Server, see the *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*.

For more information about the policies:

- “Lightweight mode policy”

Lightweight mode policy

Know the policy that you can set to enable the lightweight mode and where to find and set this policy, description, and values.



pid_ts_lightweight_mode

Location	Registry Editor > HKEY_LOCAL_MACHINE > SOFTWARE > IBM > ISAM ESSO > Deployment Options
Description	Mode of AccessAgent to use for a remote session on terminal server.
Registry	[D0] "TSLightweightMode"
Type	DWORD
Values	<ul style="list-style-type: none">• #0: Does not enable lightweight mode• #1: Enables lightweight mode (default value)• #2: Enforces lightweight mode
Scope	Machine
Note	Refresh on use.

Chapter 10. Policies for Debugging Management and Control

Use the debugging management and control policies to manage settings for troubleshooting, auditing, network, and maintenance.

See “AccessAgent policies” on page 56 for more details about network policies.

For more information:

- “Auditing policies”
- “Network policies” on page 108
- “Troubleshooting policies”
- “Temporary file policy” on page 47
- “Log policies” on page 47

Auditing policies

Know the different AccessAudit policies, where to find and set these policies, their descriptions, and their default values.



pid_audit_custom_events_list

IMS Entry	List of custom audit event codes and their corresponding display names
Location	AccessAdmin > System > System policies > AccessAudit Policies
Description	List of custom audit event codes and their corresponding display names. Entry format is: event_code,display_name. Custom event code values start from 0x43015000 to 0x43015FFF. Note: AccessProfiles must be written to detect the events and submit appropriate custom audit logs.
Registry	
Type	String list
Values	
Scope	System
Note	Each custom event is represented by one string of the form: event_code, display_name. Event_code must be a hexadecimal value in the range: 0x43015000 to 0x43015FFF You can select multiple values.

Troubleshooting policies

Know the policies that are usually configured during troubleshooting, where to find and set these policies, their descriptions, and their default values.



pid_wallet_sync_manual_enabled

Location	Registry Editor > HKEY_LOCAL_MACHINE > SOFTWARE > IBM > ISAM ESSO > Temp
-----------------	--

 **pid_wallet_sync_manual_enabled**

Description	Whether to enable the Synchronize with IMS option by right-clicking on the AccessAgent icon in WNA.
Registry	[T] "WalletSyncManualEnabled"
Type	DWORD
Values	<ul style="list-style-type: none"> • #0: No (default value) • #1: Yes
Scope	Machine
Note	Refreshed on use.

 **pid_wallet_delete_enabled**

Location	Registry Editor > HKEY_LOCAL_MACHINE > SOFTWARE > IBM > ISAM ESSO > Temp
Description	<p>Whether to enable a Delete user Wallets option by right-clicking on the AccessAgent icon in WNA.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. This menu item is only available when no user is logged on to AccessAgent. 2. This menu item deletes all user Wallets, but not the machine Wallet. 3. If this feature is used on a Citrix or Terminal Server or a workstation with Local User Session Management (LUSM) enabled, make sure that only one desktop session is running when you delete the Wallets. If multiple sessions are running, the AccessAgent running in other sessions after deleting the Wallets might be unstable.
Registry	[T] "WalletDeleteEnabled"
Type	DWORD
Values	<ul style="list-style-type: none"> • #0: No (default value) • #1: Yes
Scope	Machine
Note	Refreshed on use.

 **pid_machine_policy_override_enabled**

Location	Registry Editor > HKEY_LOCAL_MACHINE > SOFTWARE > IBM > ISAM ESSO > Temp
Description	<p>Whether to override machine policies using registry values.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. If enabled, machine policies can be overridden for this machine by specifying their values in the registry key [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\DeploymentOptions]. For example, pid_second_factors_supported_list can be specified using the registry value SecondFactorsSupportedList. 2. This temporary policy is useful for troubleshooting, especially if there is no Administrator access to the IMS Server. Do not enable this policy after testing is completed so that the machine can continue to be managed through AccessAdmin. 3. This policy does not affect pid_wallet_cache_security_enabled.
Registry	[T] "MachinePolicyOverrideEnabled"

pid_machine_policy_override_enabled

Type	DWORD
Values	<ul style="list-style-type: none">• #0: No (default value)• #1: Yes
Scope	Machine
Note	Refreshed on use.

Temporary file policy

Know the policy about temporary files and where to find and set this policy, description, and values.

pid_temp_path

Location	Registry Editor > HKEY_LOCAL_MACHINE > SOFTWARE > IBM > ISAM ESSO > DeploymentOptions
Description	Path to a folder that contains the temporary files.
Registry	[D0] "TempPath"
Type	SZ
Values	<ProgramDir>\temp (default value)
Scope	Machine
Note	Refreshed on use.

Log policies

Know the different policies for logs, where to find and set these policies, their descriptions, and their default values.

pid_log_file_count

Location	Registry Editor > HKEY_LOCAL_MACHINE > SOFTWARE > IBM > ISAM ESSO > DeploymentOptions
Description	Maximum number of AccessAgent log files allowed. If the maximum number of log files is reached, the oldest log file is deleted to give priority for the new log file.
Registry	[D0] "LogFileCount"
Type	DWORD
Values	10 (default value)
Scope	Machine
Note	Refreshed on use.

pid_log_file_size

Location	Registry Editor > HKEY_LOCAL_MACHINE > SOFTWARE > IBM > ISAM ESSO > DeploymentOptions
Description	Maximum size of the log file in KB (AccessAgent.log). If the maximum file size is reached, the file is renamed, and a file is created to store the new logs.

 **pid_log_file_size**

Registry	[D0] "LogFileSize"
Type	DWORD
Values	1024 (default value)
Scope	Machine
Note	Refreshed on use.

 **pid_log_level**

Location	Registry Editor > HKEY_LOCAL_MACHINE > SOFTWARE > IBM > ISAM ESSO > DeploymentOptions
Description	Level of log details.
Registry	[D0] "LogLevel"
Type	DWORD
Values	<ul style="list-style-type: none">• #0: No logging• #1: Severe errors only (default value)• #2: Basic info• #3: More info, including SOAP logs• #4: Debugging info, including SOAP logs
Scope	Machine
Note	Refreshed on use.

 **pid_log_path**

Location	Registry Editor > HKEY_LOCAL_MACHINE > SOFTWARE > IBM > ISAM ESSO > DeploymentOptions
Description	Path to a folder that contains the AccessAgent logs.
Registry	[D0] "LogPath"
Type	SZ
Values	<ProgramDir>\logs (default value)
Scope	Machine
Note	Refreshed on use.

Note: Observer logs can be found at **Registry Editor > HKEY_LOCAL_MACHINE > SOFTWARE > IBM > ISAM ESSO > ECSS > DeploymentOptions**.

Chapter 11. Policies for Wallet and AccessAgent

Use Wallet and AccessAgent policies to configure the behavior of the Wallet and AccessAgent.

For more information:

- “Wallet policies”
- “AccessAgent policies” on page 56

Wallet policies

Know the different Wallet policies, where to find and set these policies, their descriptions, and their default values.



pid_wallet_enterprise_app_never_option_enabled

IMS Entry	Enable 'Never' for enterprise authentication services?
Location	<ul style="list-style-type: none">• AccessAdmin > User Policy Templates > New template > Create new policy template > Wallet Policies• AccessAdmin > System > System policies > Wallet Policies
Description	Whether the Never password entry option is enabled for enterprise authentication services. If the user policy is defined, it overrides the system policy.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none">• #True: Yes (default value)• #False: No
Scope	User System
Note	Refreshed on sync.



pid_wallet_personal_app_sso_enabled

IMS Entry	Enable single sign-on for personal authentication services?
Location	<ul style="list-style-type: none">• AccessAdmin > User Policy Templates > New template > Create new policy template > Wallet Policies• AccessAdmin > System > System policies > Wallet Policies
Description	Whether to enable single sign-on for personal authentication services.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none">• #True: Yes (default value)• #False: No
Scope	User System



pid_wallet_personal_app_sso_enabled

Note	Refreshed on sync.
------	--------------------



pid_accessagent_pwd_display_option

IMS Entry	Option for displaying application passwords in AccessAgent
Location	AccessAdmin > User Policy Templates > New template > Create new policy template > Wallet Policies
Description	Option for displaying application passwords in the Wallet Manager of AccessAgent through the Show password option. Note: 1. The user is asked to enter a password before the display of the application passwords. 2. Displaying application passwords is not enabled if the user is logged on using a fingerprint or smart card.
Registry	
Type	Non-negative integer
Values	<ul style="list-style-type: none"> • #0: Disallow displaying passwords. (default value) • #1: Allow displaying personal passwords. • #2: Allow displaying both enterprise and personal passwords.
Scope	User
Note	Refreshed on sync



pid_accessagent_pwd_export_option

IMS Entry	Option for exporting application passwords in AccessAgent
Location	AccessAdmin > User Policy Templates > New template > Create new policy template > Wallet Policies
Description	Option for exporting application passwords in the Wallet Manager of AccessAgent through the Export? option. Note: The user is asked to enter password before the user can export passwords.
Registry	
Type	Non-negative integer
Values	<ul style="list-style-type: none"> • #0: Disallow exporting passwords. (default value) • #1: Allow exporting personal passwords. • #2: Allow exporting both enterprise and personal passwords.
Scope	User
Note	Refreshed on sync.



pid_sso_user_control_enabled

IMS Entry	Allow user to enable or not enable single sign-on?
Location	AccessAdmin > User Policy Templates > New template > Create new policy template > Wallet Policies



pid_sso_user_control_enabled

Description	Whether to allow the user to enable or not enable single sign-on. Note: If this policy is not enabled, the Enable single sign-on and Disable single sign-on options do not display in the AccessAgent UI.
Registry	[D0] "SsoUserControlEnabled"
Type	DWORD Boolean
Values	<ul style="list-style-type: none"> • #True: Yes (default value) • #False: No
Scope	Machine User
Note	Refreshed on sync.



pid_wallet_editable_items_list

IMS Entry	List of Wallet items that can be edited by the user through AccessAgent
Location	AccessAdmin > User Policy Templates > New template > Create new policy template > Wallet Policies
Description	Displays the list of Wallet items that can be edited through AccessAgent.
Registry	
Type	
Values	<ul style="list-style-type: none"> • #1: Password • #2: Password entry option • #4: Application settings • #8: Delete credential • #16: Add credential
Scope	User
Note	



pid_wallet_cache_max

IMS Entry	Maximum number of cached Wallets
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > Wallet Policies

 **pid_wallet_cache_max**

Description	Maximum number of cached Wallets that are allowed on the machine. Note: <ol style="list-style-type: none"> 1. If the maximum limit of cached Wallets is reached, the least recently used cached Wallet is deleted before a new Wallet is cached. 2. Setting a limit on the number of cached Wallets for a shared workstation might improve logon performance. 3. If biometric authentication is used on a shared workstation, the limit on the number of cached Wallets is set to a certain value. The value is such that the possibility of false acceptance for the biometric device is negligible. False acceptance might lead to a user that logs on to the wrong Wallet. 4. Use this policy with pid_wallet_cache_max_inactivity_days so that the deleted cached Wallets can be automatically revoked on the IMS Server. 5. In some deployments, it might not be advisable to enable Wallet caching on shared workstations for security reasons. Set this policy to 0 so caching on a particular machine is not enabled. In this case, it overrides pid_wallet_caching_option.
Registry	[D0] "WalletCacheMax"
Type	DWORD
Values	999999999 (default value)
Scope	Machine
Note	<ul style="list-style-type: none"> • Set to 0 so caching is not enabled. • The maximum limit is 999999999. • Refreshed on use.

 **pid_wallet_sync_before_logon_enabled**

IMS Entry	Enable Wallet synchronization before logon?
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > Wallet Policies
Description	Whether to enable AccessAgent to synchronize with the IMS Server before logon to the Wallet. Note: If this policy is set to 1, AccessAgent synchronizes with the IMS Server: <ul style="list-style-type: none"> • before logging on to Windows (for ESSO GINA log on) • before running the logon script (for desktop logon and logon from an unlock screen)
Registry	[D0] "WalletSyncBeforeLogonEnabled"
Type	DWORD
Values	<ul style="list-style-type: none"> • #True: Yes (default value) • #False: No
Scope	Machine
Note	Refreshed on use.

 **pid_wallet_cache_security_enabled**

IMS Entry	Enable cached Wallet security?
------------------	--------------------------------



pid_wallet_cache_security_enabled

Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > Wallet Policies
Description	Whether to enable cached Wallet security. Note: <ol style="list-style-type: none"> 1. If enabled, the user and machine cached Wallets are tied to the machine where they are created. The cached Wallets that are copied from another machine fail to work. 2. Do not enable this policy if cached Wallets are shared among several machines. For example, AccessAgent on Citrix servers might be configured to access the same network folder for storing cached Wallets. 3. This policy does not affect pid_machine_policy_override_enabled.
Registry	[D0] "WalletCacheSecurityEnabled"
Type	DWORD
Values	<ul style="list-style-type: none"> • #True: Yes • #False: No (default value)
Scope	Machine
Note	Refreshed on startup.



pid_wallet_caching_option

IMS Entry	Wallet caching option
Location	AccessAdmin > System > System policies > Wallet Policies
Description	Option to control the caching of Wallets. Note: <ol style="list-style-type: none"> 1. Offline reset capability is automatically enabled if Wallet is cached. 2. Wallet is always cached on a Citrix or Terminal Server. 3. If ESSO Network Provider is used, the Wallet is cached when this policy is set to ask user or always cache. 4. Wallet is always cached if a user logs on with a smart card, hybrid smart card, or fingerprint.
Registry	
Type	Non-negative integer
Values	<ul style="list-style-type: none"> • #0: Disallow caching • #1: Ask user (default value) • #2: Always cache
Scope	System, Machine
Note	Refreshed on sync.



pid_wallet_cache_max_inactivity_days

IMS Entry	Maximum period of inactivity, in days, allowed for a cached Wallet
Location	AccessAdmin > System > System policies > Wallet Policies


pid_wallet_cache_max_inactivity_days

Description	<p>Maximum period of inactivity, in days, allowed for a cached Wallet. After the specified period, the cached Wallet is automatically revoked.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. The cached Wallet is automatically revoked on the IMS Server if it exceeded the maximum number of days for inactivity. AccessAgent automatically revokes expired cached Wallets during each periodic synchronization, and while a user is logged on to AccessAgent. 2. Inactivity is measured from the last synchronization time. Even if the user logs on to a cached Wallet every day, it can still be revoked. The cached Wallet is revoked if it is not synchronized with the IMS Server for an extended time. 3. If a cached Wallet is revoked, the user can log on only if the IMS Server is available. There must be no prompt that the Wallet is revoked. The option to cache the Wallet depends on pid_wallet_caching_option.
Registry	
Type	Positive integer
Values	999999999 (default value)
Scope	System
Note	<ul style="list-style-type: none"> • Set to 999999999 for infinity; cached Wallets do not expire. • Refreshed on sync.


pid_wallet_sync_mins

IMS Entry	Interval, in minutes, for the Wallet synchronization with the IMS Server
Location	AccessAdmin > System > System policies > Wallet Policies
Description	Interval, in minutes, for the periodic synchronization of the Wallet with the IMS Server. Synchronization is also done when the user logs on to AccessAgent.
Registry	
Type	Positive integer
Values	30 (default value)
Scope	System
Note	Refreshed on sync.


pid_wallet_open_max_tries

IMS Entry	Maximum number of consecutive invalid offline logons before the cached Wallet is locked out
Location	AccessAdmin > System > System policies > Wallet Policies
Description	Maximum number of allowed attempts with wrong offline logon before the cached Wallet is locked out.
Registry	
Type	Positive integer
Values	5 (default value)
Scope	System


pid_wallet_open_max_tries

Note	Refreshed on sync.
-------------	--------------------


pid_wallet_inject_pwd_entry_option_default

IMS Entry	Default single sign-on password entry option
Location	AccessAdmin > System > System policies > Wallet Policies
Description	Default single sign-on password entry option.
Registry	
Type	Positive integer
Values	<ul style="list-style-type: none"> • #1: Automatic log on • #2: Always (default value) • #3: Ask • #4: Never
Scope	System
Note	Refreshed on sync.


pid_sso_auto_learn_enabled

IMS Entry	Enable auto-learning?
Location	AccessAdmin > System > System policies > Wallet Policies
Description	Whether auto-learning can be enabled for single sign-on to applications.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none"> • #True: Yes (default value) • #False: No
Scope	System
Note	Refreshed on sync.


pid_migration_stage

IMS Entry	Stage of migration from version 1.x to 3.x
Location	AccessAdmin > System > System policies > Wallet Policies
Description	<p>Whether migration from Tivoli® Information Archive Manager version 1.x to 3.x is in progress and if applicable, the current stage of migration.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. The migration involves the upgrade of the IMS Server, AccessAgent, and Wallets of the users. 2. When the IMS Server is upgraded, the installer automatically sets the policy value to 1. 3. The Administrator must manually set this policy to 2 when all AccessAgent installations are upgraded. 4. The Wallets are upgraded as and when the user logs on using the upgraded AccessAgent. After all Wallets are upgraded, the policy must be set to 0 to optimize the IMS Server and AccessAgent performance.

 pid_migration_stage

Registry	
Type	Non-negative integer
Values	<ul style="list-style-type: none"> • #0: No migration or migration completed. (default value) • #1: Upgrading ISAM ESSO IMS Server and AccessAgent. • #2: ISAM ESSO IMS Server and AccessAgent fully upgraded.
Scope	System
Note	Refreshed on sync.

 pid_wallet_cleanup_on_caching_enabled

IMS Entry	
Location	Registry Editor > HKEY_LOCAL_MACHINE > SOFTWARE > IBM > ISAM ESSO > DeploymentOptions
Description	<p>Whether to do a Wallet cleanup activity every time a new Wallet is cached.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. The time to cache new Wallet can take longer than expected. 2. Set this policy to 0 for machines with many cached Wallets. 3. If the policy is set to 0: <ol style="list-style-type: none"> a. Logon to a cached Wallet when the IMS Server is offline is still slow, unless the IMS Server is set for high availability. b. If cleanup is not initiated, and the IMS Server is offline: <ul style="list-style-type: none"> • When a user is deleted, the old Wallet of the user is still on the Citrix server. • If the user caches a new Wallet (same user name), the user might not log on to the cached Wallet successfully. The user might not be able to log on because AccessAgent might access the old Wallet. The old Wallet has a different password from the new Wallet. • Run SOCIPruner.exe on a periodic basis to run cleanup.
Registry	[D0] "WalletCleanupOnCachingEnabled"
Type	DWORD
Values	<ul style="list-style-type: none"> • #0: disabled • #1: enabled
Scope	Machine
Note	

AccessAgent policies

View the details of the different policies that you can set for AccessAgent.

You can configure the following policies for AccessAgent:

- “Display policies” on page 57
- “ESSO GINA policies” on page 59
- “Desktop inactivity policies” on page 63
- “Lock and Unlock policies” on page 66
- “Smart card policies” on page 74

- “Hybrid smart card policies” on page 75
- “RFID policies” on page 79
- “Fingerprint policies” on page 85
- “Terminal Server policies” on page 88
- “Roaming session policies” on page 94
- “Log on/Log off policies” on page 95
- “Hot Key policies” on page 101
- “Emergency Hot Key policies” on page 105
- “Audit logging policies” on page 107
- “Background authentication policies” on page 107

Display policies

Know the different display policies, where to find and set these policies, their descriptions, and their default values.



pid_aa_tray_bubble_display_enabled

IMS Entry	Enable bubble pop-ups?
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Display Policies
Description	Whether to enable the bubble pop-up notification of AccessAgent at the Windows notification area.
Registry	[D0] "AATrayBubbleDisplayEnabled"
Type	Boolean DWORD
Values	<ul style="list-style-type: none"> • #True: Yes (default value) • #False: No
Scope	Machine
Note	Refreshed on use.



pid_aa_tray_menu_options_enabled

IMS Entry	Enable right-click menu options?
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Display Policies
Description	Whether to display menu options when the user right-clicks the AccessAgent icon at the Windows notification area.
Registry	
Type	
Values	<ul style="list-style-type: none"> • #True: Yes (default value) • #False: No
Scope	Machine
Note	

 **pid_session_info_display_freq_secs**

IMS Entry	Interval, in seconds, for displaying session information in bubble pop-ups
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Display Policies
Description	Frequency for displaying the AccessAgent session information in a bubble pop-up at the Windows notification area. The bubble pops up after every interval, in seconds, specified by this policy. Do not enable this feature by setting it to 0. Note: <ol style="list-style-type: none"> 1. Effective only if pid_aa_tray_bubble_display_enabled is 1. 2. Set policy to 0 to hide the session information. 3. This policy is effective if the value is greater than 15 seconds. If the value is less than 15 seconds, the pop-up is displayed continuously. 4. The displayed user name format is determined by pid_logon_user_name_display_option. 5. If the user is logged on with an Active Proximity Badge, a warning is shown in the same bubble pop-up if battery is low. 6. Modifying this policy requires a computer restart to implement the changes.
Registry	[D0] "SessionInfoDisplayFreqSecs"
Type	DWORD
Values	0 (default value)
Scope	Machine
Note	<ul style="list-style-type: none"> • Set to 0 for no display. • Refreshed on startup.

 **pid_aa_feedback_link**

IMS Entry	AccessAgent Feedback link
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Display Policies
Description	Enables the Feedback link in the AccessAgent user interface, which launches an email client or web browser. Note: <ul style="list-style-type: none"> • If the policy value is blank, (default) AccessAgent does not show the Feedback link. • If the policy value format is mailto:abc@example.com, clicking Feedback launches the default email client of the user and the email is sent to abc@example.com. • If the policy value format is http://example.com, clicking Feedback launches the default browser of the user and navigates to http://example.com.
Registry	[D0] "AAFeedbackLink"
Type	String SZ
Values	
Scope	Machine
Note	Refreshed on sync.

pid_ims_server_name

Location	Registry Editor > HKEY_LOCAL_MACHINE > SOFTWARE > IBM > ISAM ESSO > IMSService > DefaultIMSSettings
Description	Default IMS Server name.
Registry	[DIMS] "ImsServerName"
Type	SZ
Values	
Scope	Machine
Note	Refreshed when set using the Set IMS Server Location utility.

ESSO GINA policies


Know the different policies for ESSO GINA, where to find and set these policies, their descriptions, and their default values.

pid_engina_winlogon_option_enabled

IMS Entry	Allow logon bypass through Windows?
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > ESSO GINA Policies
Description	Whether to enable the option to go to Windows Logon directly from ESSO GINA.
Registry	[D0] "EnginaWinlogonOptionEnabled"
Type	DWORD
Values	<ul style="list-style-type: none">• #1: Yes (default value)• #0: No
Scope	Machine
Note	Refreshed on use.

pid_engina_app_launch_enabled

IMS Entry	Enable application launch from ESSO GINA?
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > ESSO GINA Policies
Description	Whether to enable the launching of an application from the ESSO GINA welcome or locked screen. Note: This policy is not supported when Transparent Screen Lock is enabled.
Registry	[D0] "EnginaAppLaunchEnabled"
Type	DWORD
Values	<ul style="list-style-type: none">• #1: Yes• #0: No (default value)
Scope	Machine
Note	Refreshed on use.

 **pid_engina_app_launch_label**

IMS Entry	Display label for application launch
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > ESSO GINA Policies
Description	Display label for the link on ESSO GINA welcome or locked screen, for launching an application. Note: <ul style="list-style-type: none"> • Effective only if pid_engina_app_launch_enabled is 1. • This policy is not supported when Transparent Screen Lock is enabled.
Registry	[D0] "EnginaAppLaunchLabel"
Type	SZ
Values	
Scope	Machine
Note	Refreshed on use.

 **pid_engina_app_launch_cmd**

IMS Entry	Command line for application launch
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > ESSO GINA Policies
Description	Command line for launching an application from an ESSO GINA welcome or locked screen. Note: <ol style="list-style-type: none"> 1. Effective only if pid_engina_app_launch_enabled is 1. 2. If the application is launched from a welcome screen, the owner of the process for the application is System. 3. If the application is launched from a locked screen, the owner of the process for the application is currently logged on desktop user. 4. This policy is not supported when Transparent Screen Lock is enabled.
Registry	[D0] "EnginaAppLaunchCmd"
Type	SZ
Values	
Scope	Machine
Note	Refreshed on use.

  **pid_engina_bypass_hot_key_enabled**

IMS Entry	Enable ESSO GINA Bypass Hot Key?
Location	<ul style="list-style-type: none"> • AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > ESSO GINA Policies • AccessAdmin > System > System policies > AccessAgent Policies > ESSO GINA Policies



pid_engina_bypass_hot_key_enabled

Description	Whether the ESSO GINA Bypass Hot Key is enabled. Note: <ol style="list-style-type: none"> 1. If enabled, the user can press the ESSO GINA Bypass Hot Key sequence to bypass ESSO GINA and go to Windows to log on or unlock. 2. The Hot Key is accepted at any of the following ESSO GINA states: Welcome, Log On, Computer Locked, Unlock This Computer. 3. If the Hot Key is pressed at the computer locked screen, AccessAgent does not ask the user for confirmation on whether to log off the previous user. Microsoft GINA is presented to the user, but the unlocking is only for the same user or Administrator. 4. This policy is not effective if local user session management is enabled (for example, pid_lum_sessions_max is greater than 1). 5. Modifying this policy requires a machine restart to implement the changes.
Registry	[D0] "EnginaBypassHotKeyEnabled"
Type	DWORD Boolean
Values	<ul style="list-style-type: none"> • #1: Yes (default value) • #0: No • #1: True (default value) • #0: False
Scope	Machine System
Note	Refreshed on startup.



pid_engina_bypass_hot_key_sequence

IMS Entry	ESSO GINA Bypass Hot Key sequence
Location	<ul style="list-style-type: none"> • AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > ESSO GINA Policies • AccessAdmin > System > System policies > AccessAgent Policies > ESSO GINA Policies
Description	The ESSO GINA Bypass Hot Key sequence. Maximum of 3 keys from the set: {Ctrl, Shift, Alt, Ins, Del, Home, End, PgUp, PgDn, Break, E}. Note: <ol style="list-style-type: none"> 1. Effective only if pid_engina_bypass_hot_key_enabled is enabled. 2. Modifying this policy requires a machine restart to implement the changes.
Registry	[D0] "EnginaBypassHotKeySequence"
Type	MULTI_SZ String list
Values	<ul style="list-style-type: none"> • Ctrl • Alt • Home


pid_engina_bypass_hot_key_sequence

Scope	Machine System
Note	<p>You can select a maximum of three keys from this set except Ctrl+Alt+Del:</p> <ul style="list-style-type: none"> • Ctrl • Shift • Alt • Ins • Del • Home • End • PgUp • PgDn • Break • E <p>2 of the keys in this set must be used so that the probability of conflict with other applications is minimized: Ctrl, Shift, Alt</p> <p>Refreshed on startup.</p>


pid_engina_bypass_automatic_enabled

IMS Entry	Enable automatic ESSO GINA bypass?
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > ESSO GINA Policies
Description	<p>Whether automatic ESSO GINA Bypass is enabled.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. If this policy is enabled, the IMS Server is not accessible, and the user Wallet is not cached, AccessAgent automatically bypasses ESSO GINA. Microsoft GINA is displayed when the user attempts to log on or unlock the machine. The user is prompted with a configurable text message (pid_engina_bypass_automatic_text). 2. If pid_unlock_option is 4, AccessAgent prompts whether to log off the previous user. If the user clicks Yes and: <ul style="list-style-type: none"> • pid_enc_pwd_is_ad_pwd_enabled is True • IMS Server is not accessible • Wallet of the user is not cached <p>AccessAgent prompts the user with a configurable text message (pid_engina_bypass_automatic_text). If the user clicks OK, AccessAgent logs off the previous desktop of the user and automatically redirects the new user to the Microsoft GINA logon screen.</p> 3. This feature does not support logon with second factors. 4. Modifying this policy requires a machine restart to implement the changes.
Registry	[D0] "EnginaBypassAutomaticEnabled"
Type	DWORD
Values	<ul style="list-style-type: none"> • #1: Yes • #0: No (default value)

 pid_engina_bypass_automatic_enabled

Scope	Machine
Note	Refreshed on startup.

Desktop inactivity policies

Know the different policies for desktop inactivity, where to find and set these policies, their descriptions, and their default values.

  pid_desktop_inactivity_mins

IMS Entry	Desktop inactivity duration, in minutes
Location	<ul style="list-style-type: none"> • AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Desktop Inactivity Policies • AccessAdmin > System > System policies > AccessAgent Policies > Desktop Inactivity Policies
Description	Desktop inactivity duration, in minutes, after which AccessAgent can do a set of actions.
Registry	[D0] "DesktopInactivityMins"
Type	DWORD Positive integer
Values	30 (default value)
Scope	Machine System
Note	<ul style="list-style-type: none"> • Refreshed on sync for system policy. • Refreshed on use for machine policy.

  pid_desktop_inactivity_action

IMS Entry	Desktop inactivity actions
Location	<ul style="list-style-type: none"> • AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Desktop Inactivity Policies • AccessAdmin > System > System policies > AccessAgent Policies > Desktop Inactivity Policies
Description	<p>Actions to be done by AccessAgent after a period of desktop inactivity.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. This policy is not effective if the computer is already locked. In that case, the locked inactivity action is effective. 2. If the user is not logged on to a Wallet, the log off Wallet actions for policy values 2 and 5 is not performed. 3. If No action is selected, an active and open default desktop takes effect upon inactivity timeout. 4. If other values are selected excluding No action, an active and open default desktop locks the screen upon inactivity timeout.
Registry	[D0] "DesktopInactivityAction"


pid_desktop_inactivity_action

Type	DWORD Non-negative integer
Values	<ul style="list-style-type: none"> • #0: No action (default value) • #1: Log off Windows • #2: Log off Wallet • #4: Lock computer • #5: Log off Wallet and lock computer
Scope	Machine System
Note	<ul style="list-style-type: none"> • Refreshed on sync for system policy. • Refreshed on use for machine policy.


pid_desktop_inactivity_action_countdown_secs

IMS Entry	Confirmation countdown duration, in seconds, for desktop inactivity
Location	<ul style="list-style-type: none"> • AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Desktop Inactivity Policies • AccessAdmin > System > System policies > AccessAgent Policies > Desktop Inactivity Policies
Description	Confirmation countdown duration, in seconds, for desktop inactivity. Set the value to 0 to disable confirmation countdown.
Registry	[D0] "DesktopInactivityActionCountdownSecs"
Type	DWORD Non-negative integer
Values	5 (default value)
Scope	Machine System
Note	<ul style="list-style-type: none"> • Set to 0 to turn off confirmation countdown. • Refreshed on sync for system policy. • Refreshed on use for machine policy.


pid_win_screensaver_action

IMS Entry	Actions on Windows screen saver activation
Location	<ul style="list-style-type: none"> • AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Desktop Inactivity Policies • AccessAdmin > System > System policies > AccessAgent Policies > Desktop Inactivity Policies



pid_win_screensaver_action

Description	<p>Actions to be done by AccessAgent on Windows screen saver activation.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. This policy is only effective if at least one user is logged on to AccessAgent. 2. If this policy triggers a computer lock, desktop inactivity action becomes ineffective. 3. If this policy triggers a screen saver without password protection, the desktop inactivity action remains effective when the screen saver is on. 4. This policy accepts two-level desktop inactivity behavior. If: <ul style="list-style-type: none"> • this policy is set to 1 • the desktop inactivity minutes is set to 4 • the Windows screen saver is set to time out in 2 minutes and not password protected <p>Then, the computer does the following actions:</p> <ul style="list-style-type: none"> • shows the screen saver after 2 minutes of no user activity • locks the computer after an additional 2 minutes of no user activity <p>Important: The screensaver action is not supported in Microsoft Windows 7 or later.</p>
Registry	[D0] "WinScreensaverAction"
Type	DWORD Non-negative integer
Values	<ul style="list-style-type: none"> • #0: Disable Windows screen saver • #1: If screen saver is password protected, lock computer, else show normal screen saver • #2: Lock computer (default value)
Scope	Machine System
Note	<ul style="list-style-type: none"> • Refreshed on sync for system policy. • Refreshed on use for machine policy. <p>AccessAgent assumes that ScreenSaverGracePeriod is 0 when it locks the computer and screen saver activation. If the user dismisses the screensaver before the grace period is over, the computer remains unlocked, but the lock scripts are run.</p>



pid_locked_computer_inactivity_mins

IMS Entry	Locked computer inactivity duration, in minutes
Location	<ul style="list-style-type: none"> • AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Desktop Inactivity Policies • AccessAdmin > System > System policies > AccessAgent Policies > Desktop Inactivity Policies
Description	Locked computer inactivity duration, in minutes, after which AccessAgent can perform a set of actions.
Registry	[D0] "LockedComputerInactivityMins"



pid_locked_computer_inactivity_mins

Type	DWORD Positive integer
Values	30 (default value)
Scope	Machine System
Note	<ul style="list-style-type: none"> • Refreshed on sync for system policy. • Refreshed on use for machine policy.



pid_locked_computer_inactivity_action

IMS Entry	Locked computer inactivity actions when the user is logged on to the Wallet
Location	<ul style="list-style-type: none"> • AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Desktop Inactivity Policies • AccessAdmin > System > System policies > AccessAgent Policies > Desktop Inactivity Policies
Description	<p>Actions to be done by AccessAgent after a period of desktop inactivity while the computer is locked and the user is logged on to the Wallet.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. Effective only if pid_lusm_sessions_max is 1. 2. This policy is effective only if the ESSO GINA screen lock is shown.
Registry	[D0] "LockedComputerInactivityAction"
Type	DWORD Non-negative integer
Values	<ul style="list-style-type: none"> • #0: No action (default value) • #1: Log off Windows
Scope	Machine System
Note	<ul style="list-style-type: none"> • Refreshed on sync for system policy. • Refreshed on use for machine policy.

Lock and Unlock policies

Know the different lock and unlock policies, where to find and set these policies, their descriptions, and their default values.



pid_script_lock_enabled

IMS Entry	Enable lock script during locking of the user's AccessAgent session?
Location	AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > Lock/Unlock Policies



pid_script_lock_enabled

Description	<p>Whether to enable running the lock script when locking the AccessAgent session of the user.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. The lock script is run only if the session of the user is visible during locking. In Local User Session Management (LUSM), currently invisible user sessions do not have the lock script executed. 2. The lock script is run regardless of whether there is desktop inactivity or locking is manually triggered. For example, pressing Win+L or tapping an RFID card. 3. The lock script is useful for closing applications when locking a guest AccessAgent session. The lock script can also be used with the unlock script in a Local User Session Management scenario to record any single-instance application that might: <ul style="list-style-type: none"> • be running before lock. • be relaunched during unlock. <p>Important:</p> <p>When using Microsoft Windows 7 or later:</p> <ul style="list-style-type: none"> • The lock script is run after the computer locks instead of before the computer locks. • The user is not prompted for action upon computer lock. <p>Blocking lock scripts are not supported. The scripts are expected to perform non-blocking actions. For instance, a message box prompt in the script is not supported.</p>
Registry	
Type	Boolean
Values	<ul style="list-style-type: none"> • #True: Yes • #False: No (default value)
Scope	User
Note	Refreshed on sync.


pid_script_lock_type

IMS Entry	Lock script type
Location	AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > Lock/Unlock Policies
Description	<p>Type of lock script to run.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. Effective only if pid_script_lock_enabled is enabled. 2. See pid_script_lock_enabled.
Registry	
Type	Positive integer
Values	<ul style="list-style-type: none"> • #1: Batch (default) • #2: VBScript
Scope	User
Note	Refreshed on sync.



pid_script_lock_code

IMS Entry	Lock script code
Location	AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > Lock/Unlock Policies
Description	Source code of lock script to run. Note: 1. Effective only if pid_script_lock_enabled is enabled. 2. See pid_script_lock_enabled.
Registry	
Type	String
Values	
Scope	User
Note	Refreshed on sync.



pid_script_unlock_enabled

IMS Entry	Enable unlock script when user unlocks an existing AccessAgent session?
Location	AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > Lock/Unlock Policies
Description	Whether to enable the running of the unlock script when the user unlocks an existing AccessAgent session. Note: 1. The unlock script is run only if the user has an existing AccessAgent session and is unlocking the session. 2. The unlock script is not run if the user is unlocking a shared workstation that is: <ul style="list-style-type: none"> • logged on with a generic Windows account and • not currently logged on to AccessAgent In this case, the logon script (pid_script_logon_enabled) is run instead. 3. The unlock script can be used in Local User Session Management. The script can automatically launch single-instance applications that might be terminated by other users who are logged on to the same workstation. 4. The unlock script is not supported if pid_lock_option is 2 (such as transparent screen lock is used).
Registry	
Type	Boolean
Values	<ul style="list-style-type: none"> • #True: Yes • #False: No (default value)
Scope	User
Note	Refreshed on sync.



pid_script_unlock_type

IMS Entry	Unlock script type
------------------	--------------------



pid_script_unlock_type

Location	AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > Lock/Unlock Policies
Description	Type of unlock script to run. Note: 1. Effective only if pid_script_unlock_enabled is enabled. 2. See pid_script_unlock_enabled.
Registry	
Type	Positive integer
Values	<ul style="list-style-type: none"> • #1: Batch (default) • #2: VBScript
Scope	User
Note	Refreshed on sync.




pid_script_unlock_code

IMS Entry	Unlock script code
Location	AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > Lock/Unlock Policies
Description	Source code of unlock script to run. Note: 1. Effective only if pid_script_unlock_enabled is enabled. 2. See pid_script_unlock_enabled.
Registry	
Type	String
Values	
Scope	User
Note	Refreshed on sync.



pid_unlock_option

IMS Entry	Unlock computer policy
Location	<ul style="list-style-type: none"> • AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > Lock/Unlock Policies • AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Lock/Unlock Policies

 **pid_unlock_option**

Description	<p>Unlock computer policy for controlling who can unlock a computer when it is locked by a user who is logged on to AccessAgent. Same user refers to the same user who locked the computer. Administrator refers to the Windows user with Administrator privilege on that computer. The Wallet must contain the Windows credentials of an Administrator user on that computer.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. Effective only if pid_lusm_sessions_max is 1. 2. This policy is ignored if pid_lock_option is 2 (transparent screen lock). In transparent screen lock mode, any user can unlock the computer. 3. If the policy is set to 3 and a different user tries to unlock the computer, AccessAgent unlocks the computer and displays the current desktop. However, AccessAgent logs on the user to a new Wallet. 4. If the policy is set to 4, only the same user can unlock the computer and return to the current desktop. For other users, AccessAgent logs off from the old desktop and logs on to the new Wallet. AccessAgent does not require a user to present a second factor. If a new Wallet does not have a desktop account on the computer, the user must log on to Windows. This option is not supported for smart card. <p>Important: Limitations for Microsoft Windows 7 or later versions:</p> <ul style="list-style-type: none"> • Option 3 works only with a Shared Desktop. • Option 4 logs off the current AccessAgent logon session without attempting to log on again as a second user.
Registry	[D0] "UnlockOption"
Type	DWORD Positive integer
Values	<ul style="list-style-type: none"> • #1: Only the same user can unlock • #3: Any user with or without current desktop account Wallet can unlock (default value) • #4: Only the same user can unlock, but different user can re-log on to Windows
Scope	Machine User
Note	<ul style="list-style-type: none"> • Refreshed on sync for user policy. • Refreshed on use for machine policy.

 **pid_unlock_different_user_action_countdown_secs**

IMS Entry	Confirmation countdown duration, in seconds, for unlocking by a different user
Location	<ul style="list-style-type: none"> • AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > Lock/Unlock Policies • AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Lock/Unlock Policies



pid_unlock_different_user_action_countdown_secs

Description	Confirmation countdown duration, in seconds, for unlocking by a different user. Set the value to 0 to disable confirmation countdown Note: <ol style="list-style-type: none"> 1. Effective only if pid_lusm_sessions_max is 2. 2. Effective when a user attempts to unlock a computer when another user is already logged on to AccessAgent. 3. If the policy value is not 0, the user can click the prompt to cancel the switch user. If the user does not confirm, AccessAgent proceeds to unlock the computer.
Registry	[D0] "UnlockDifferentUserActionCountdownSecs"
Type	DWORD Non-negative integer
Values	0: to not enable confirmation countdown
Scope	Machine User
Note	<ul style="list-style-type: none"> • Refreshed on sync for user policy. • Refreshed on use for machine policy.



pid_lock_option

IMS Entry	Screen lock option
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Lock/Unlock Policies
Description	Type of screen lock to be used when the computer is locked. Note: <ol style="list-style-type: none"> 1. If pid_lusm_sessions_max is greater than 1, only policy 1 (ESSO GINA screen lock) is supported. 2. From a transparent screen lock, the user can unlock the computer or switch to another user by presenting a second factor. 3. From a transparent screen lock, the AccessAgent UI is displayed when the IBM Security Access Manager for Enterprise Single Sign-On Hot Key is pressed. From this screen, the user can manually log off from AccessAgent, which unlocks the computer, and does the actions that are specified by pid_logoff_manual_action. The logoff action is available regardless of the setting for pid_logoff_manual_when_locked_option_enabled. 4. Even after transparent screen lock is activated, the action that is specified by pid_desktop_inactivity_action is still carried out after the period of desktop inactivity elapsed. Then, set pid_desktop_inactivity_action to 4.
Registry	[D0] "LockOption"
Type	DWORD
Values	<ul style="list-style-type: none"> • #1: ESSO GINA screen lock (default) • #2: Transparent screen lock
Scope	Machine
Note	Refreshed on use.

 **pid_lock_transparent_text**

IMS Entry	Transparent screen lock message
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Lock/Unlock Policies
Description	Configurable text for transparent screen lock. Note: Effective only if pid_lock_option is 2.
Registry	[D0] "LockTransparentText"
Type	SZ
Values	Tap your RFID card or Ctrl-Alt-E to unlock. (default value)
Scope	Machine
Note	The text box can contain up to 40 characters. Refreshed on use.

 **pid_lock_transparent_hot_key_enabled**

IMS Entry	Enable transparent screen lock hot key?
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Lock/Unlock Policies
Description	Whether the Ctrl-Esc Hot Key sequence is enabled during transparent screen lock. Note: <ol style="list-style-type: none">1. Effective only if pid_lock_option is 2 and transparent screen lock is shown.2. If enabled, this Hot Key is equivalent to the IBM Security Access Manager for Enterprise Single Sign-On Hot Key when the computer is locked. When pressed, the AccessAgent UI is shown on the transparent screen lock.3. This additional Hot Key is useful for remote access systems (for example, LANDesk) that can send only limited key sequences.
Registry	[D0] "LockTransparentHotKeyEnabled"
Type	DWORD
Values	<ul style="list-style-type: none">• #1: Yes• #0: No (default value)
Scope	Machine
Note	Refreshed on use.

 **pid_unlock_with_win_option**

IMS Entry	Option for allowing unlock bypass through Windows
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Lock/Unlock Policies

pid_unlock_with_win_option

Description	Option for unlocking the computer with Windows unlock. Note: <ol style="list-style-type: none">1. Set the policy to 1 for personal workstations, and 2 for shared workstations.2. Set the policy to 0 if pid_lusm_sessions_max is greater than 1.3. AccessAgent is logged off when the computer is unlocked with Windows unlock.
Registry	[D0] "UnlockWithWinOption"
Type	DWORD
Values	<ul style="list-style-type: none">• Disabled• Windows unlock is always available (default)• Windows unlock is available only if AccessAgent is not logged on
Scope	Machine
Note	Refreshed on use.

pid_unlock_user_name_prefill_option

IMS Entry	User name prefill option for unlock prompt
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Lock/Unlock Policies
Description	Option for pre-filling the AccessAgent unlock prompt with a user name. <ul style="list-style-type: none">• For policy value 0, the setting for pid_logon_user_name_prefill_option applies to the unlock prompt.• For policy value 1, if a user is logged on to AccessAgent, the unlock prompt is pre-filled with the currently logged on user name. If no user is logged on to AccessAgent, the unlock prompt is pre-filled with last logged on user name.• This policy is not applicable to private desktop (pid_lusm_sessions_max is greater than 1).
Registry	[D0] "UnlockUserNamePrefillOption"
Type	DWORD
Values	<ul style="list-style-type: none">• #0: Use the user name pre-fill option for logon prompt (default value)• #1: Prefill with currently logged on or last logged on user name
Scope	Machine
Note	Refreshed on use.

pid_fast_unlock_enabled

IMS Entry	Enable fast unlock without IMS Server check?
Location	AccessAdmin > Machine Policy Templates > New template > AccessAgent Policies > Lock/Unlock Policies
Description	Whether to allow AccessAgent to unlock a computer using a second authentication factor, without any checks with the IMS Server.
Registry	
Type	Boolean

 **pid_fast_unlock_enabled**

Values	<ul style="list-style-type: none"> • #0: Fast unlock is not enabled • #1: Fast unlock is enabled (default value)
Scope	Machine
Note	

Smart card policies

Know the different smart card policies, where to find and set these policies, their descriptions, and their default values.

  **pid_sc_removal_action**

IMS Entry	Smart card removal actions
Location	<ul style="list-style-type: none"> • AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > Smart card Policies • AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Smart card Policies
Description	Actions to be done when a smart card is removed.
Registry	
Type	Non-negative integer
Values	<ul style="list-style-type: none"> • #1: Log off Windows • #2: Log off Wallet • #4: Lock computer (default value) • #5: Log off Wallet and lock computer
Scope	Machine User
Note	

 **pid_sc_win_logon_enabled**

IMS Entry	Enable Windows smart card logon?
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Smart card Policies
Description	<p>Whether to allow smart card users to log on to Windows through certificate-based authentication.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. If enabled, after the user logs on to AccessAgent from the Welcome screen, the user can log on to Windows with the smart card certificate. 2. This policy is only applicable if the pid_engina_ui_enabled policy is set. This policy is not supported on Windows 7 or later versions.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none"> • #True: Yes • #False: No (default value)

 **pid_sc_win_logon_enabled**

Scope	Machine
Note	Refreshed on sync.

**pid_sc_map_cert_to_entdir_acc_enabled**

IMS Entry	Enable automatic mapping of certificate to the enterprise directory account during sign up?
Location	AccessAdmin > System > System policies > AccessAgent Policies > Smart card Policies
Description	Whether to automatically identify the enterprise directory account by using the smart card certificate attributes during sign-up. The user is not prompted to provide a user name during sign-up.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none">• #True: Yes• #False: No (default value)
Scope	System
Note	Refreshed on sync.

**pid_engina_ui_enabled**



IMS Entry	Enable the ISAM ESSO UI when Windows is logged off or locked?
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Smart card Policies
Description	Whether to display the IBM Security Access Manager for Enterprise Single Sign-On UI instead of the Windows UI when Windows is logged off or locked.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none">• #True: Yes (default value)• #False: No
Scope	Machine
Note	Refreshed on sync.

Hybrid smart card policies

Know the different smart card policies, where to find and set these policies, their descriptions, and their default values.

**pid_sc_1f_unlock_enabled**


IMS Entry	Enable single factor smart card unlock?
Location	AccessAdmin > Machine Policy Templates > New Template > AccessAgent Policies > Smart card Policies AccessAdmin > User Policy Template > New Template > AccessAgent Policies > Smart card Policies

  **pid_sc_1f_unlock_enabled**

Description	Whether to allow a single factor smart card unlock without PIN by the same user who locked the computer, if unlock happens within a specified duration.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none"> • #True: Yes • #False: No (default value)
Scope	Machine User
Note	

  **pid_sc_1f_unlock_timeout_secs**

IMS Entry	Time expiry, in seconds, for single factor smart card unlock
Location	AccessAdmin > Machine Policy Templates > New Template > AccessAgent Policies > Smart card Policies AccessAdmin > User Policy Template > New Template > AccessAgent Policies > Smart card Policies
Description	Time expiry, in seconds, for a single factor smart card unlock. After a duration has passed from last lock, single factor smart card unlock is not allowed.
Registry	
Type	Non-negative integer
Values	<ul style="list-style-type: none"> • >0: Grace period in seconds • 0: Grace period is infinite (default value)
Scope	Machine User
Note	

 **pid_sc_1f_logon_enable**

IMS Entry	Enable single factor smart card logon?
Location	AccessAdmin > Machine Policy Templates > New Template > AccessAgent Policies > Smart card Policies
Description	Whether to allow a single factor smart card logon without a PIN by a user who recently logged on using smart card and PIN on the same computer or another computer. This policy applies if logon happens in the duration that is specified by the single factor smart card logon timeout.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none"> • #True: Yes • #False: No (default value)
Scope	Machine
Note	



pid_sc_1f_logon_timeout_mins

IMS Entry	Time expiry, in minutes, for single factor smart card logon
Location	AccessAdmin > User Policy Template > New Template > AccessAgent Policies > Smart card Policies
Description	Time expiry, in minutes, for single factor smart card logon. After this duration (timed from last logon with smart card and PIN), single factor smart card logon is not allowed.
Registry	
Type	Non-negative integer
Values	<ul style="list-style-type: none"> • >0: Grace period in minutes • 0: Invalid. Single factor smart card logon is Not enabled.
Scope	User
Note	



pid_sc_1f_logon_extension_allowed

IMS Entry	Extend single factor smart card logon time expiry when user logs on with smart card and PIN?
Location	AccessAdmin > User Policy Template > New Template > AccessAgent Policies > Smart card Policies
Description	Whether to extend the time expiry for single factor smart card logon when the user logs on with a smart card and PIN before grace period expires.
Registry	
Type	
Values	<ul style="list-style-type: none"> • No • Yes
Scope	Machine User
Note	



pid_sc_present_same_action

IMS Entry	Actions on the desktop for using the same smart card if user logged on with single factor
Location	AccessAdmin > Machine Policy Templates > New Template > AccessAgent Policies > Smart card Policies AccessAdmin > User Policy Template > New Template > AccessAgent Policies > Smart card Policies
Description	Actions on the desktop for using the same smart card. This policy is effective only if the current user session starts with a single factor smart card logon.
Registry	
Type	Non-negative integer

  **pid_sc_present_same_action**

Values	<ul style="list-style-type: none"> • #0: No action • #1: Log off Windows • #2: Log off Wallet • #4: Lock computer (default value) • #5: Log off Wallet and lock computer
Scope	Machine User
Note	

  **pid_sc_present_same_action_countdown_secs**

IMS Entry	Confirmation countdown duration, in seconds, on the desktop, for using the same smart card
Location	AccessAdmin > Machine Policy Templates > New Template > AccessAgent Policies > Smart card Policies AccessAdmin > User Policy Template > New Template > AccessAgent Policies > Smart card Policies
Description	Confirmation countdown duration, in seconds, on the desktop, for using the same smart card
Registry	
Type	Non-negative integer
Values	<ul style="list-style-type: none"> • 0: No countdown • >0: Countdown in seconds <p>Note: 5 is the default value.</p>
Scope	Machine User
Note	

  **pid_sc_present_different_action**

IMS Entry	Actions on the desktop for using a different smart card if the user logged on with single factor
Location	AccessAdmin > Machine Policy Templates > New Template > AccessAgent Policies > Smart card Policies AccessAdmin > User Policy Template > New Template > AccessAgent Policies > Smart card Policies
Description	Actions on the desktop for using a different smart card. This policy is effective only if the current user session starts with a single factor smart card logon.
Registry	
Type	Non-negative integer
Values	<ul style="list-style-type: none"> • #0: No action • #4: Lock computer • #5: Log off Wallet and lock computer • #6: Switch user (default value) • #8: Log off Windows and log on as new user

 **pid_sc_present_different_action**

Scope	Machine User
Note	

 **pid_sc_present_different_action_countdown_secs**

IMS Entry	Confirmation countdown duration, in seconds, on the desktop, for using a different smart card
Location	AccessAdmin > Machine Policy Templates > New Template > AccessAgent Policies > Smart card Policies AccessAdmin > User Policy Template > New Template > AccessAgent Policies > Smart card Policies
Description	Confirmation countdown duration, in seconds, on the desktop, for using a different smart card
Registry	
Type	Non-negative integer
Values	<ul style="list-style-type: none"> • 0: No countdown • >0: Countdown in seconds Note: 5 is the default value.
Scope	Machine User
Note	

RFID policies

Know the different RFID policies, where to find and set these policies, their descriptions, and their default values.

RFID policies

 **pid_rfid_tap_same_action**

IMS Entry	Actions on the desktop for tapping same RFID
Location	<ul style="list-style-type: none"> • AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > RFID Policies • AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > RFID Policies
Description	Actions to be done by AccessAgent on the desktop when the currently logged on user taps his RFID card Note: <ol style="list-style-type: none"> 1. This policy is not applicable if the user did not log on using an RFID. 2. If pid_lusm_sessions_max is greater than 1, AccessAgent with the policy value 1 (Log off Windows) logs off the desktop session of the user and shows the computer locked screen.
Registry	[D0] "RfidTapSameAction"

  **pid_rfid_tap_same_action**

Type	DWORD Non-negative integer
Values	<ul style="list-style-type: none"> • #0: No action (default value) • #1: Log off Windows • #2: Log off Wallet • #4: Lock computer • #5: Log off Wallet and lock computer
Scope	Machine User
Note	<ul style="list-style-type: none"> • Refreshed on sync for user policy. • Refreshed on use for machine policy.

  **pid_rfid_tap_same_action_countdown_secs**

IMS Entry	Confirmation countdown duration in seconds, on the desktop, for tapping same RFID on the card reader
Location	<ul style="list-style-type: none"> • AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > RFID Policies • AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > RFID Policies
Description	Confirmation countdown duration in seconds, on the desktop, for tapping same RFID on the card reader. Set the value to 0 to disable confirmation countdown.
Registry	[D0] "RfidTapSameActionCountdownSecs"
Type	DWORD Non-negative integer
Values	5 (default value)
Scope	Machine User
Note	<ul style="list-style-type: none"> • Set to 0 to not enable confirmation countdown. However, do not set value to 0 to prevent an accidental double detection of an RFID tap. • Refreshed on sync for user policy. • Refreshed on use for machine policy.

  **pid_rfid_only_unlock_enabled**

IMS Entry	Enable RFID-only unlock?
Location	<ul style="list-style-type: none"> • AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > RFID Policies • AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > RFID Policies

 **pid_rfid_only_unlock_enabled**

Description	Whether to allow RFID-only unlock (without password) by the same user who locked the computer, if unlock happens in a specified duration.
Registry	[D0] "RfidOnlyUnlockEnabled"
Type	DWORD Boolean
Values	<ul style="list-style-type: none"> • #1: Yes • #0: No (default value)
Scope	Machine User
Note	<ul style="list-style-type: none"> • Refreshed on sync for user policy. • Refreshed on use for machine policy.

 **pid_rfid_only_unlock_timeout_secs**

IMS Entry	Time expiry, in seconds, for RFID-only unlock
Location	<ul style="list-style-type: none"> • AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > RFID Policies • AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > RFID Policies
Description	<p>Time expiry, in seconds, for an RFID-only unlock. After this duration (timed from the last lock), RFID-only unlock is not allowed.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. Effective only if pid_rfid_only_unlock_enabled is enabled. 2. Also applies to Active Proximity Badge.
Registry	[D0] "RfidOnlyUnlockTimeoutSecs"
Type	DWORD Non-negative integer
Values	0 (default value)
Scope	Machine User
Note	<ul style="list-style-type: none"> • Set value to 0 to not enable expiry and always enable RFID-only unlock. • Refreshed on sync for user policy. • Refreshed on use for machine policy.

 **pid_rfid_only_logon_timeout_mins**

IMS Entry	Time expiry, in minutes, for RFID-only logon
Location	AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > RFID Policies

 **pid_rfid_only_logon_timeout_mins**

Description	Time expiry, in minutes, for RFID-only logon. After this duration (timed from the last logon with an RFID and password), RFID-only logon is not allowed. Note: <ol style="list-style-type: none"> 1. Effective only if pid_rfid_only_logon_enabled is enabled. 2. Timeout is refreshed upon every logon to the IMS Server with an RFID and password.
Registry	
Type	Non-negative integer
Values	480 (default value)
Scope	User
Note	<ul style="list-style-type: none"> • Set value to 0 if RFID-only logon is not enabled. • Refreshed on sync.

 **pid_rfid_tap_different_action**

IMS Entry	Actions on the desktop for tapping different RFID
Location	<ul style="list-style-type: none"> • AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > RFID Policies • AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > RFID Policies
Description	<p>Actions to be done by AccessAgent on the desktop when an RFID card that does not belong to the currently logged on user is tapped on the card reader.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. If pid_rfid_display_utility_enabled is 1, this policy is not effective. 2. This policy is applicable even if the current user did not use an RFID to log on. 3. For policy value 8, AccessAgent does not require the new user to tap the RFID again after logoff from Windows. 4. If pid_lusm_sessions_max is greater than 1, AccessAgent with a policy value of 1 (Log off Windows) logs off the desktop session of the user. The computer locked screen is displayed. AccessAgent with a policy value of 6 (Switch user) attempts to create a user desktop session for the new user. AccessAgent with a policy value of 8 (Log off Windows and log on as a new user) logs off the desktop session of the current user and creates a user desktop session for the new user. 5. Switching of a user is only supported for users who use the same type of second factor. 6. If pid_rfid_tap_different_action has the value of Switch user, and pid_win_fast_user_switching_enabled is enabled, fast user switching takes place. <p>Important: Limitation for Microsoft Windows Windows 7 or later versions: For the value Log off Windows and log on as new user, AccessAgent logs off the current logon session without attempting to log on again as a second user.</p>
Registry	[D0] "RfidTapDifferentAction"

 **pid_rfid_tap_different_action**

Type	DWORD Non-negative integer
Values	<ul style="list-style-type: none"> • #0: No action (default value) • #4: Lock computer • #5: Log off Wallet and lock computer • #6: Switch user • #8: Log off Windows and log on as new user
Scope	Machine User
Note	<ul style="list-style-type: none"> • Refreshed on sync for user policy. • Refreshed on use for machine policy.

 **pid_rfid_tap_different_action_countdown_secs**

IMS Entry	Confirmation countdown duration in seconds, on the desktop, for tapping different RFID on the card reader
Location	<ul style="list-style-type: none"> • AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > RFID Policies • AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > RFID Policies
Description	Confirmation countdown duration in seconds, on the desktop, for tapping different RFID on the card reader. Set the value to 0 to disable confirmation countdown.
Registry	[D0] "RfidTapDifferentActionCountdownSecs"
Type	DWORD Non-negative integer
Values	5 (default value)
Scope	Machine User
Note	<ul style="list-style-type: none"> • Set value to 0 if confirmation countdown is not enabled. Set to this value only when RFID tap different action is 6 to prevent an accidental double detection of an RFID tap. • Refreshed on sync for user policy. • Refreshed on use for machine policy.

 **pid_rfid_only_logon_enabled**

IMS Entry	Enable RFID-only logon?
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > RFID Policies

 **pid_rfid_only_logon_enabled**

Description	<p>Whether to allow RFID-only logon (without password) by a user who recently logged on using an RFID and password on the same or another computer, if logon happens within the duration that is specified by the RFID-only logon time-out (pid_rfid_only_logon_timeout_mins)</p> <p>Note:</p> <ol style="list-style-type: none"> 1. RFID-only logon works only if the IMS Server is online and the user has an existing cached Wallet on the computer. 2. RFID-only logon is tied to the specific RFID card used for logon. If the user has two RFID cards, and the first card is logged on, the user can log on only with the first RFID card. If the user attempts to log on with the second RFID card, the user must be prompted for a password. 3. For better security, pid_wallet_cache_max_inactivity_days must be set to clear inactive Wallets. 4. RFID-only logon is not supported if pid_lusm_sessions_max is greater than 1. 5. ARFID is not applicable. 6. Either condition is applicable if both RFID-only unlock and RFID-only logon features are enabled: <ul style="list-style-type: none"> • If a logged on user locks the computer: When the user taps an RFID card to unlock the existing session, the RFID-only unlock feature is invoked. During unlock, a password is required if the RFID-only unlock timeout expired. • If no user is logged on and the computer is locked: When a user tap an RFID card to unlock the computer, the RFID-only logon feature is invoked. During logon, a password is required if the conditions specified in the policy for RFID-only logon are not met.
Registry	[D0] "RfidOnlyLogonEnabled"
Type	DWORD
Values	<ul style="list-style-type: none"> • #1: Yes • #0: No (default value)
Scope	Machine
Note	Refreshed on use.

 **pid_rfid_display_utility_enabled**

IMS Entry	Enable RFID display utility?
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > RFID Policies
Description	<p>Whether to display the registration status of an RFID card that does not belong to the currently logged on user when it is tapped on the desktop.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. If the policy value is 1, the policy overrides pid_rfid_tap_different_action. If the RFID card is registered, the user name is displayed in a prompt. 2. This display utility works only when a user is logged on to AccessAgent.
Registry	[D0] "RfidDisplayUtilityEnabled"
Type	DWORD

 **pid_rfid_display_utility_enabled**

Values	<ul style="list-style-type: none"> • #1: Yes • #0: No (default value)
Scope	Machine
Note	Refreshed on use.

Fingerprint policies

Know the different fingerprint policies, where to find and set these policies, their descriptions, and their default values.

 **pid_fingerprint_tap_same_action**

IMS Entry	Actions on the desktop for tapping the same finger
Location	<ul style="list-style-type: none"> • AccessAdmin > User Policy Templates > AccessAgent Policies > Fingerprint Policies • AccessAdmin > Machine Policy Templates > AccessAgent Policies > Fingerprint Policies
Description	<p>Actions to be done by AccessAgent on the desktop when the currently logged on user taps a finger on the fingerprint reader.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. This policy is not applicable if the user did not log on using a fingerprint. 2. Currently, this policy is supported only if pid_lusm_sessions_max is 1. If pid_lusm_sessions_max is set to greater than 1, AccessAgent with a policy value of 1 (Log off Windows) logs off the user from the desktop session and shows the computer locked screen.
Registry	[D0] "FingerprintTapSameAction"
Type	DWORD Non-negative integer
Values	<ul style="list-style-type: none"> • #0: No action (default value) • #1: Log off Windows • #2: Log off Wallet • #4: Lock computer • #5: Log off Wallet and lock computer
Scope	Machine User
Note	<ul style="list-style-type: none"> • Refreshed on sync for user policy. • Refreshed on use for machine policy.

 **pid_fingerprint_tap_same_action_countdown_secs**

IMS Entry	Confirmation countdown duration, in seconds, on the desktop, for tapping the same finger on the fingerprint reader
------------------	--



pid_fingerprint_tap_same_action_countdown_secs

Location	<ul style="list-style-type: none"> • AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > Fingerprint Policies • AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Fingerprint Policies
Description	Confirmation countdown duration, in seconds, on the desktop, for tapping the same finger on the fingerprint reader. Set the value to 0 to disable confirmation countdown.
Registry	[D0] "FingerprintTapSameActionCountdownSecs"
Type	DWORD Non-negative integer
Values	5 (default value)
Scope	Machine User
Note	<ul style="list-style-type: none"> • If you do not want to enable confirmation countdown, set value to 0. However, do not set to this value to prevent an accidental double detection of a finger tap. • Refreshed on sync for user policy. • Refreshed on use for machine policy.



pid_fingerprint_tap_different_action

IMS Entry	Actions on the desktop for tapping a different finger
Location	<ul style="list-style-type: none"> • AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > Fingerprint Policies • AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Fingerprint Policies
Description	<p>Actions to be done by AccessAgent on the desktop when a finger that does not belong to the currently logged on user is tapped on the fingerprint reader.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. This policy is applicable even if the current user did not use a fingerprint to log on. 2. For policy value 8, AccessAgent does not require the new user to tap a fingerprint again after log off from Windows. 3. This policy is supported only if pid_lusm_sessions_max is 1. If pid_lusm_sessions_max is set to greater than 1, AccessAgent with a policy value 1 (Log off Windows) logs off the user from the desktop session. The computer locked screen is displayed. AccessAgent with a policy value of 6 (Switch user) attempts to create a user desktop session for the new user. AccessAgent with a policy value of 8 (Log off Windows and log on as new user) logs off the current user from the desktop session and creates a user desktop session for the new user. <p>Important: Limitation for Microsoft Windows 7 or later versions: For option 8, AccessAgent logs off the current logon session without attempting to log on again as a second user.</p>



pid_fingerprint_tap_different_action

Registry	[D0] "FingerprintTap DifferentAction"
Type	DWORD Non-negative integer
Values	<ul style="list-style-type: none"> • #0: No action (default value) • #4: Lock computer • #5: Log off Wallet and lock computer • #6: Switch user • #8: Log off Windows and log on as new user
Scope	Machine User
Note	<ul style="list-style-type: none"> • Refreshed on sync for user policy. • Refreshed on use for machine policy.




pid_fingerprint_tap_different_action_countdown_secs

IMS Entry	Confirmation countdown duration, in seconds, on the desktop, for tapping a different finger on the fingerprint reader
Location	<ul style="list-style-type: none"> • AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > Fingerprint Policies • AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Fingerprint Policies
Description	Confirmation countdown duration, in seconds, on the desktop, for tapping a different finger on the fingerprint reader. Set the value to 0 to disable confirmation countdown.
Registry	[D0] "FingerprintTapDifferentActionCountdownSecs"
Type	DWORD Non-negative integer
Values	5 (default value) 0 (not enable confirmation countdown)
Scope	Machine User
Note	<ul style="list-style-type: none"> • If you do not want to enable confirmation countdown, set the value to 0. However, set to this value only when fingerprint tap different action is 6 to prevent an accidental double detection of a finger tap. • Refreshed on sync for user policy. • Refreshed on use for machine policy.



pid_fingerprint_registration_max

IMS Entry	Maximum number of fingerprints that can be registered per user
------------------	--

 **pid_fingerprint_registration_max**

Location	AccessAdmin > System > System policies > AccessAgent Policies > Fingerprint Policies
Description	Maximum number of fingerprints that each user is allowed to register. Note: A user who exceeded the maximum number of registered fingerprints can log on with any of the registered fingerprints if the value of this policy is reduced. However, to register a new fingerprint, an existing fingerprint has to be replaced. The user cannot increase the number of registered fingerprints.
Registry	
Type	Positive integer
Values	1 (default)
Scope	System
Note	<ul style="list-style-type: none"> You can specify a minimum of one registered fingerprint, and a maximum of 10 registered fingerprints. Refreshed on sync.

 **pid_fast_logon_enabled**

IMS Entry	Enable fast logon using cached Wallet without authenticating with the IMS Server?
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Fingerprint Policies
Description	Users with cached Wallets can log on to AccessAgent without authenticating with the IMS Server. The fingerprint that is used to log on is validated against the IMS Server after AccessAgent connects to the desktop. To do authentication after logon, enable background authentication.
Registry	
Type	Positive integer
Values	<ul style="list-style-type: none"> Yes (default value) No
Scope	Machine
Note	<ul style="list-style-type: none"> If pid_fast_logon_enabled is set to Yes, and pid_background_auth_enabled is set to 1, AccessAgent checks the IMS Server for the validity of the scanned fingerprint. If the fingerprint is revoked, the user is logged off from the session. If pid_fast_logon_enabled is set to Yes, and pid_background_auth_enabled is set to 0, AccessAgent does not check with the IMS Server for the validity of the scanned fingerprint. A user can still log on to the Windows desktop with a revoked fingerprint.

Terminal Server policies

Know the different terminal server policies, where to find and set these policies, their descriptions, and their default values.

 **pid_ts_logon_prompt_enabled**

IMS Entry	Enable auto-launching of AccessAgent log on prompt?
------------------	---

 **pid_ts_logon_prompt_enabled**

Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Terminal Server Policies
Description	Whether to launch the AccessAgent logon dialog if the user is not logged on to AccessAgent while a Terminal Server session or Citrix application is launched. Note: This policy must be set on the remote AccessAgent (such as on the Terminal Server or Citrix server).
Registry	[D0] "TSLogonPromptEnabled"
Type	DWORD
Values	<ul style="list-style-type: none"> • #1: Yes • #0: No (default value)
Scope	Machine
Note	Refreshed on use.

 **pid_ts_engina_logon_no_local_session_enabled**

IMS Entry	Use ESSO GINA log on when there is no local AccessAgent session?
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Terminal Server Policies
Description	Whether to use ESSO GINA logon or Microsoft GINA logon for the Terminal Server session, when there is no local AccessAgent session. Note: <ol style="list-style-type: none"> 1. This policy must be set on the remote AccessAgent (such as on the Terminal Server or Citrix server). 2. Set the policy to 0 on Citrix servers.
Registry	[D0] "TSEnginaLogonNoLocalSessionEnabled"
Type	DWORD
Values	<ul style="list-style-type: none"> • #1: Yes • #0: No (default value)
Scope	Machine
Note	Refreshed on use.

 **pid_ts_aa_menu_option**

IMS Entry	Option for displaying menu options on the remote AccessAgent
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Terminal Server Policies

 **pid_ts_aa_menu_option**

Description	Whether to display menu options on the AccessAgent user interface in a Terminal Server or Citrix session. Note: 1. If the policy value is 1, only Remote session information is displayed when there is a local AccessAgent session. Full menu options are displayed when there is no local AccessAgent session. The same scenario applies to right-click menu options for the AccessAgent icon at the Windows notification area. 2. If the policy value is 2, all menu options are displayed except for Lock this computer when there is a local AccessAgent session. Full menu options are displayed when there is no local AccessAgent session. The same scenario applies to right-click menu options for the AccessAgent icon at the Windows notification area. Use this option for Roaming Desktop configurations.
Registry	[D0] "TSAaMenuOption"
Type	DWORD
Values	<ul style="list-style-type: none"> • Display menu options only if there is no local AccessAgent sessions (default value) • Always display all menu options
Scope	Machine
Note	

 **pid_com_redir_enabled**

IMS Entry	Enable COM port redirection?
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Terminal Server Policies
Description	Whether the device monitoring mechanism can do a COM port redirection from the client machine (connecting to the Terminal Server) to the Terminal Server. Note: 1. If redirection is enabled for AccessAgent on Terminal Server or Citrix server, authentication devices on remote client machines can be monitored. For example, thin clients with no AccessAgent installed can be monitored. AccessAgent maps a virtual COM port (pid_com_redir_local_virtual_port) on the Terminal Server or Citrix server to a physical COM port (pid_com_redir_remote_physical_port) on the remote client. 2. Modifying this policy requires a computer restart to implement the changes.
Registry	[D0] "ComRedirEnabled"
Type	DWORD
Values	<ul style="list-style-type: none"> • #1: Yes • #0: No (default value)
Scope	Machine
Note	Refreshed on startup.

 **pid_com_redir_local_virtual_port**

IMS Entry	Virtual COM port on the Terminal Server
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Terminal Server Policies
Description	Virtual COM port on the Terminal Server to which data from the client COM port is redirected. Note: Effective only if pid_com_redir_enabled is 1.
Registry	[D0] "ComRedirLocalVirtualPort"
Type	DWORD
Values	1 (default value)
Scope	Machine
Note	<ul style="list-style-type: none">• The value can range from 1 to 8.• Refreshed on startup.

 **pid_com_redir_remote_physical_port**

IMS Entry	Physical COM port on the client machine
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Terminal Server Policies
Description	Physical COM port on the client to which the authentication device (for example, RFID reader) is connected. The redirection takes place from this port to the virtual COM port of the Terminal Server. Note: <ol style="list-style-type: none">1. Effective only if pid_com_redir_enabled is 1.2. Modifying this policy requires a computer restart to implement the changes.
Registry	[D0] "ComRedirRemotePhysicalPort"
Type	DWORD
Values	1 (default value)
Scope	Machine
Note	<ul style="list-style-type: none">• The minimum value is 1.• Refreshed on startup.

 **pid_ts_start_aa_no_local_aa_enabled**

Location	Registry Editor > HKEY_LOCAL_MACHINE > SOFTWARE > IBM > ISAM ESSO > DeploymentOptions
-----------------	---

 **pid_ts_start_aa_no_local_aa_enabled**

Description	Whether to start remote AccessAgent while a published application is launched through Terminal Server or Citrix, and if a local AccessAgent is not present. Note: <ol style="list-style-type: none"> 1. This policy must be set on the remote AccessAgent (such as on the Terminal Server or Citrix server). 2. This policy applies to launching of published applications only. If a remote desktop is launched, the remote AccessAgent is always started. 3. For a policy value of 0, users cannot log on to a remote AccessAgent from computers that do not have a local AccessAgent installed (for example, home or Internet café).
Registry	[D0] "TSstartAANoLocalAAEnabled"
Type	DWORD
Values	<ul style="list-style-type: none"> • #1: Yes (default value) • #0: No
Scope	Machine
Note	Refreshed on use.

 **pid_machine_type_ts**

Location	Registry Editor > HKEY_LOCAL_MACHINE > SOFTWARE > IBM > ISAM ESSO > DeploymentOptions
Description	Whether the machine is a Terminal Server or Citrix server. Note: <ol style="list-style-type: none"> 1. This policy must be set to 1 on the remote AccessAgent (such as, on the Terminal Server or Citrix server). 2. If this policy is set to 1, AccessAgent behaves as a remote AccessAgent: <ul style="list-style-type: none"> • It synchronizes itself with the local AccessAgent. • The second factors supported list is not effective. It is treated as an empty list. • Lock computer options from the WNA and AccessAgent UI are not enabled, if log on to remote AccessAgent uses credentials that are submitted by local AccessAgent. • It uses a Terminal Service second factor bypass option to determine its behavior when the authentication policy of the user requires a second factor for logon. 3. The following combinations of policy settings are not supported (behavior is unpredictable): <ul style="list-style-type: none"> • policy value 0 on a Terminal Server or Citrix server installation. • policy value 1 on a client machine installation. <p>Modifying this policy requires a computer restart to implement the changes.</p>
Registry	[D0] "MachineTypeTS"
Type	DWORD
Values	<ul style="list-style-type: none"> • #1: Machine is Terminal Server • #0: Machine is not Terminal Server (default value)
Scope	Machine
Note	Refreshed on startup.

 pid_ts_delay_app_launch_exe_list

Location	Registry Editor > HKEY_LOCAL_MACHINE > SOFTWARE > IBM > ISAM ESSO > DeploymentOptions
Description	The list of applications which are delayed from launching until the remote AccessAgent is ready to do single sign-on. Note: <ol style="list-style-type: none"> 1. This policy must be set on the remote AccessAgent (such as on the Citrix server). 2. Effective only if pid_ts_delay_app_launch_enabled is enabled. 3. Each application must be indicated by its executable name (for example, notepad.exe). 4. This feature is not supported in AccessAdmin. To enable this feature, edit the values manually in the Windows registry.
Registry	[D0] "TSDelayAppLaunchExeList"
Type	MULTI_SZ
Values	
Scope	Machine
Note	Refreshed on use.

 pid_ts_delay_app_launch_enabled

Location	Registry Editor > HKEY_LOCAL_MACHINE > SOFTWARE > IBM > ISAM ESSO > ECSS > DeploymentOptions
Description	Whether to enable the delay of an application launch for the Citrix server. Note: <ol style="list-style-type: none"> 1. This feature is only applicable to Citrix. It is not applicable to Terminal Server access through RDP. 2. This policy must be set on the remote AccessAgent, such as on the Citrix server. 3. If not enabled, the user might first see the logon prompt of the application before the remote AccessAgent can do single sign-on. This result might cause some confusion to the user. Enabling this feature for an application ensures that the remote AccessAgent is ready to do single sign-on when the user sees the logon prompt. 4. This feature is only applicable to a local AccessAgent automatically logging on to a remote AccessAgent. If there is no local AccessAgent or the local AccessAgent is not logged on, application launch is not delayed even if this feature is enabled. 5. This feature is not supported in AccessAdmin. To enable this feature, edit the values manually in the Windows registry.
Registry	[D0] "TSDelayAppLaunchEnabled"
Type	DWORD
Values	<ul style="list-style-type: none"> • #1: Yes • #0: No (default value)
Scope	Machine
Note	Refreshed on use.



pid_ts_delay_app_launch_timeout_secs

Location	Registry Editor > HKEY_LOCAL_MACHINE > SOFTWARE > IBM > ISAM ESSO > DeploymentOptions
Description	Timeout, in seconds, for delaying an application launch. Note: <ol style="list-style-type: none"> 1. This policy must be set on the remote AccessAgent (such as on the Citrix server). 2. Effective only if pid_ts_delay_app_launch_enabled is enabled. 3. Remote AccessAgent first waits for a connection to be established with a local AccessAgent. If a connection is not established in the timeout duration, the application launches. 4. If a local AccessAgent manages to establish a connection with a remote AccessAgent, the remote AccessAgent waits for another timeout period for single sign-on to be ready. If a remote AccessAgent is not ready for single sign-on in the timeout duration, the application launches. 5. The user might wait up to two times the timeout duration if the local AccessAgent manages to connect with a remote AccessAgent before the lapse of the first timeout duration. 6. This feature is not supported in AccessAdmin. To enable this feature, edit the values manually in the Windows registry.
Registry	[D0] "TSDelayAppLaunchTimeoutSecs"
Type	DWORD
Values	*10
Scope	Machine
Note	Refreshed on use.

Roaming session policies

Know the different roaming session policies, where to find and set these policies, their descriptions, and their default values.



pid_ts_lock_local_computer_action

IMS Entry	Actions on remote session while locking the local computer
Location	AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > Roaming Session Policies
Description	Option to disconnect the Terminal Server or Citrix session, or log off from the remote AccessAgent while locking the local computer.
Registry	
Type	Non-negative integer
Values	<ul style="list-style-type: none"> • #0: No action (default value) • #1: Disconnect remote session • #2: Log off remote AccessAgent and disconnect remote session • #3: Log off remote session • #4: Log off remote AccessAgent
Scope	User
Note	Refreshed on sync.



pid_ts_logoff_local_session_action

IMS Entry	Actions on remote session before logging off local session
Location	AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > Roaming Session Policies
Description	Option to disconnect the Terminal Server or Citrix session, or log off from the remote AccessAgent before logoff from the local AccessAgent.
Registry	
Type	Non-negative integer
Values	<ul style="list-style-type: none"> • #0: No action • #1: Disconnect remote session • #2: Log off remote AccessAgent and disconnect remote session (default value) • #3: Log off remote session • #4: Log off remote AccessAgent
Scope	User
Note	Refreshed on sync.

Log on/Log off policies

Know the different log on and log off policies, where to find and set these policies, their descriptions, and their default values.



pid_script_logon_enabled

IMS Entry	Enable logon script during user logon?
Location	AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > Logon/Logoff Policies
Description	Whether to enable the running of a logon script during user logon.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none"> • #True: Yes • #False: No (default value)
Scope	User
Note	Refreshed on sync.



pid_script_logon_type

IMS Entry	Logon script type
Location	AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > Logon/Logoff Policies
Description	Type of logon script to run. Note: Effective only if script logon is enabled.
Registry	
Type	Positive integer



pid_script_logon_type

Values	<ul style="list-style-type: none"> Batch (default) VBScript
Scope	User
Note	Refreshed on sync.



pid_script_logon_code

IMS Entry	Logon script code
Location	AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > Logon/Logoff Policies
Description	Source code of logon script to run. Note: Effective only if script logon is enabled.
Registry	
Type	String
Values	
Scope	User
Note	Refreshed on sync.



pid_script_logoff_enabled

IMS Entry	Enable logoff script during user logoff?
Location	AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > Logon/Logoff Policies
Description	Whether to enable the running of a logoff script during user logoff.
Registry	AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > Logon/Logoff Policies
Type	Boolean
Values	<ul style="list-style-type: none"> #True: Yes #False: No (default value)
Scope	User
Note	Refreshed on sync.



pid_script_logoff_type

IMS Entry	Logoff script type
Location	AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > Logon/Logoff Policies
Description	Type of logoff script to run. Note: Effective only if script logoff is enabled.
Registry	
Type	Positive integer



pid_script_logoff_type

Values	<ul style="list-style-type: none"> • #1: Batch (default) • #2: VBScript
Scope	User
Note	Refreshed on sync.



pid_script_logoff_code

IMS Entry	Logoff script code
Location	AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > Logon/Logoff Policies
Description	Source code of logoff script to run. Note: Effective only if script logoff is enabled.
Registry	
Type	String
Values	
Scope	User
Note	Refreshed on sync.



pid_logoff_manual_enabled

IMS Entry	Allow user to manually log off AccessAgent?
Location	<ul style="list-style-type: none"> • AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > Logon/Logoff Policies • AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Logon/Logoff Policies
Description	Whether to allow the user to manually log off from AccessAgent. Note: If this policy is not enabled, the Log off AccessAgent option does not display in the AccessAgent UI.
Registry	[D0] "LogoffManualEnabled"
Type	DWORD Boolean
Values	<ul style="list-style-type: none"> • #1: Yes (default value) • #0: No • #True: Yes (default value) • #False: No
Scope	Machine User
Note	Refreshed on sync.



pid_logoff_manual_action

IMS Entry	Actions on manual logoff by user
Location	<ul style="list-style-type: none">• AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > Logon/Logoff Policies• AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Logon/Logoff Policies
Description	Actions to be done by AccessAgent on a manual logoff by the user. Note: <ol style="list-style-type: none">1. Effective when a user manually logs off from the Wallet from a desktop or transparent screen lock.2. If pid_lusm_sessions_max is greater than 1, AccessAgent with policy value 1 (Log off Windows) logs off the user from the desktop session and shows the computer locked screen. Use this policy value for Local User Session Management. If the policy value is 2, user is logged off from AccessAgent. However, the user cannot log on to AccessAgent unless Ctrl+Alt+Del is pressed to log on from the IBM Security Access Manager for Enterprise Single Sign-On replaced Windows security dialog.
Registry	[D0] "LogoffManualAction"
Type	DWORD Positive integer
Values	<ul style="list-style-type: none">• #1: Log off Windows• #2: Log off Wallet (default value)• #4: Log off Wallet and lock computer
Scope	Machine User
Note	<ul style="list-style-type: none">• Refreshed on sync for user policy.• Refreshed on use for machine policy.



pid_logoff_manual_action_countdown_secs

IMS Entry	Confirmation countdown duration, in seconds, for manual logoff by user
Location	<ul style="list-style-type: none">• AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAgent Policies > Logon/Logoff Policies• AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Logon/Logoff Policies
Description	Confirmation countdown duration, in seconds, for a manual logoff by a user. Set the value to 0 to disable confirmation countdown. Note: <ol style="list-style-type: none">1. Effective when the user manually logs off from the Wallet from a desktop or locked computer window.2. If the policy value is not zero, the user must click the prompt to confirm logoff. If the user does not confirm, AccessAgent does not proceed with the logoff.
Registry	[D0] "LogoffManualActionCountdownSecs"



pid_logoff_manual_action_countdown_secs

Type	DWORD Non-negative integer
Values	30 (default value)
Scope	Machine User
Note	<ul style="list-style-type: none"> • If you do not want to enable confirmation countdown, set the value to 0. • Refreshed on sync for user policy. • Refreshed on use for machine policy.



pid_en_network_provider_enabled

IMS Entry	Enable Network Provider?
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Logon/Logoff Policies
Description	<p>Whether to enable the Network Provider (EnNetworkProvider).</p> <p>Note:</p> <ol style="list-style-type: none"> 1. Second factor authentication is not supported by this feature. 2. Effective only if EnNetworkProvider has been installed by the AccessAgent installer. 3. If enabled, AccessAgent attempts to automatically log on to itself using the credentials provided at Microsoft GINA. It works with the Active Directory password synchronization feature so that the same password can log on to both Windows and AccessAgent.
Registry	[D0] "EnNetworkProviderEnabled"
Type	DWORD
Values	<ul style="list-style-type: none"> • #1: Yes • #0: No (default value)
Scope	Machine
Note	Refreshed on use.



pid_logon_user_name_prefill_option

IMS Entry	User name prefill option
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Logon/Logoff Policies
Description	<p>Option for pre-filling the AccessAgent Logon prompt with a user name.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. Set this policy to 0 for shared desktops with many users. 2. Set this policy to 1 for personal desktops or shared desktops with few users. 3. Set this policy to 2 for Terminal Server or Citrix Server. For policy value 2 to work properly, the following Microsoft registry value must be set to 0: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system] "dontdisplaylastusername"

 **pid_logon_user_name_prefill_option**

Registry	[D0] "LogonUserNamePrefillOption"
Type	DWORD
Values	<ul style="list-style-type: none"> • #0: Do not prefill. • #1: Prefill with last logged on user name. (default value) • #2: Prefill with currently logged on Windows user name.
Scope	Machine
Note	Refreshed on use.

 **pid_logon_user_name_display_option**

IMS Entry	User name display option
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Logon/Logoff Policies
Description	<p>Option for displaying the name of the currently logged on user.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. If this policy is set to 2 or 3, AccessAgent displays the full name of the user, obtained from Active Directory upon logon to Wallet. The machine must be logged on to a domain. If AccessAgent cannot obtain the full name from Active Directory, it reverts to displaying the user name. 2. The limited size of the UI can display about 20 characters only. If the name is truncated, it is appended with "...". 3. This policy affects the entire AccessAgent UI where the user name is displayed (for example, main UI, locked screen). 4. In a two-factor deployment (RFID, smart card, and others), the user does not need a user name to log on to AccessAgent. If the user forgets the second factor, the user must enter a user name and password to log on to AccessAgent or AccessAssistant. If the full name is always displayed, the user might forget the logon user name, because they do not use it every day and also do not see it in the AccessAgent user interface. As a best practice, policy value 1 must be used for a two-factor deployment.
Registry	[D0] "LogonUserNameDisplayOption"
Type	DWORD
Values	<ul style="list-style-type: none"> • 1 - User name (default value) • 2 - Given name followed by family name • 3 - Family name followed by given name
Scope	Machine
Note	Refreshed on logon.

 **pid_logoff_app_timeout_secs**

IMS Entry	Timeout, in seconds, for application logoff
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Logon/Logoff Policies



pid_logoff_app_timeout_secs

Description	Timeout, in seconds, for logging off from applications. Note: <ol style="list-style-type: none"> When AccessAgent logs off from a Wallet (during manual logoff or switch user), logging off from applications might occur (depends on configuration). This policy specifies a configurable timeout for logging off from applications. If an application is not terminated by its AccessProfile after the timeout, it can be terminated by setting the Terminate on time-out and time-out attributes of the gen_sign_out_trigger appropriately.
Registry	[D0] "LogoffAppTimeoutSecs"
Type	DWORD
Values	5 (default value)
Scope	Machine
Note	<ul style="list-style-type: none"> The value can range from 0 to 60. Refreshed on use.





pid_wallet_logoff_action_for_apps_default

IMS Entry	Default action for applications, when user logs off AccessAgent
Location	AccessAdmin > System > System policies > AccessAgent Policies > Logon/Logoff Policies
Description	Default action to take for all applications when the user logs off AccessAgent. To log off applications, the AccessProfile for each application must contain a logoff action, otherwise the application is not logged off. Note: <ol style="list-style-type: none"> If the policy value is 1, AccessAgent attempts to log off all applications. The AccessProfile for each application must contain a logoff action, otherwise the application is not logged off. If the policy value is 2, AccessAgent closes applications that are monitored by AccessAgent. All applications with AccessProfiles are monitored, regardless of whether AccessAgent can log on to the application. This policy is effective when a user is logged off from AccessAgent, for example, during a switch user operation.
Registry	
Type	Positive integer
Values	<ul style="list-style-type: none"> #1: Log off the application #2: Close the application #3: Do nothing (default value)
Scope	System
Note	Refreshed on sync.

Hot Key policies

Know the different hot key policies, where to find and set these policies, their descriptions, and their default values.





pid_enc_hot_key_enabled

IMS Entry	Enable ISAM ESSO Hot Key?
Location	<ul style="list-style-type: none"> • AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Hot Key Policies • AccessAdmin > System > System policies > AccessAgent Policies > Hot Key Policies
Description	<p>Whether the IBM Security Access Manager for Enterprise Single Sign-On Hot Key is enabled.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. From ESSO GINA, pressing the Hot Key displays the logon screen. 2. From a locked screen, pressing the Hot Key displays the unlock screen. 3. From a desktop, if AccessAgent is not logged on, pressing the Hot Key launches the logon screen. 4. From a desktop, if AccessAgent is logged on, the behavior of the Hot Key is defined by IBM Security Access Manager for Enterprise Single Sign-On Hot Key action.
Registry	[D0] "EncHotKeyEnabled"
Type	DWORD Boolean
Values	<ul style="list-style-type: none"> • #1: Yes (default value) • #0: No • #True: Yes (default value) • #False: No
Scope	Machine System
Note	Refreshed on startup.




pid_enc_hot_key_sequence

IMS Entry	ISAM ESSO Hot Key sequence
Location	<ul style="list-style-type: none"> • AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Hot Key Policies • AccessAdmin > System > System policies > AccessAgent Policies > Hot Key Policies
Description	<p>The IBM Security Access Manager for Enterprise Single Sign-On Hot Key sequence. Maximum of 3 keys from the set: {Ctrl, Shift, Alt, Ins, Del, Home, End, PgUp, PgDn, Break, E}.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. Effective only if pid_enc_hot_key_enabled is enabled. 2. Modifying this policy requires a computer restart to implement the changes.
Registry	[D0] "EncHotKeySequence"
Type	MULTI_SZ String list



pid_enc_hot_key_sequence

Values	<ul style="list-style-type: none"> • Ctrl • Alt • E
Scope	Machine System
Note	<ul style="list-style-type: none"> • Set a maximum of three key combinations: Ctrl, Shift, Alt, Ins, Del, Home, End, PgUp, PgDn, Break, E • Select any of these three keys to minimize the probability of conflict with other applications: Ctrl, Shift, Alt • Refreshed on startup.



pid_enc_hot_key_action

IMS Entry	ISAM ESSO Hot Key press actions at desktop when AccessAgent is logged on
Location	<ul style="list-style-type: none"> • AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Hot Key Policies • AccessAdmin > System > System policies > AccessAgent Policies > Hot Key Policies
Description	<p>Actions to be done by AccessAgent if the ISAM ESSO Hot Key is pressed from a desktop when a user is logged on to AccessAgent.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. Effective only if pid_enc_hot_key_enabled is enabled. 2. Effective only if IBM Security Access Manager for Enterprise Single Sign-On Hot Key is pressed at desktop when a user is logged on to AccessAgent. 3. If pid_lusm_sessions_max is greater than 1, AccessAgent with a policy value of 1 (Log off Windows) logs off the user from the desktop session and shows the computer locked screen.
Registry	[D0] "EncHotKeyAction"
Type	DWORD Non-negative integer
Values	<ul style="list-style-type: none"> • #0: No action • #1: Log off Windows • #2: Log off Wallet • #4: Lock computer • #5: Log off Wallet and lock computer • #9: Launch AccessAgent window (default value)
Scope	Machine System
Note	<ul style="list-style-type: none"> • Refreshed on sync for system policy. • Refreshed on use for machine policy.



pid_enc_hot_key_action_countdown_secs

IMS Entry	Confirmation countdown duration, in seconds, for pressing the ISAM ESSO Hot Key
Location	<ul style="list-style-type: none">• AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Hot Key Policies• AccessAdmin > System > System policies > AccessAgent Policies > Hot Key Policies
Description	Confirmation countdown duration, in seconds, for pressing the IBM Security Access Manager for Enterprise Single Sign-On Hot Key. Set the value to 0 to disable confirmation countdown. Note: <ol style="list-style-type: none">1. Effective only if pid_enc_hot_key_enabled is enabled.2. Effective only if IBM Security Access Manager for Enterprise Single Sign-On Hot Key is pressed when a user is logged on to AccessAgent and computer is not locked.
Registry	[D0] "EncHotKeyActionCountdownSecs"
Type	DWORD Non-negative integer
Values	5 (default value)
Scope	Machine System
Note	<ul style="list-style-type: none">• If you do not want to enable confirmation countdown, set this policy to 0.• Refreshed on sync for system policy.• Refreshed on use for machine policy.



pid_enc_hot_key_not_logged_on_action

IMS Entry	ISAM ESSO Hot Key press actions at desktop when AccessAgent is not logged on
Location	<ul style="list-style-type: none">• AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Hot Key Policies• AccessAdmin > System > System policies > AccessAgent Policies > Hot Key Policies



pid_enc_hot_key_not_logged_on_action

Description	<p>Actions to be done by AccessAgent if the IBM Security Access Manager for Enterprise Single Sign-On Hot Key is pressed at the desktop when a user is not logged on to AccessAgent.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. Effective only if pid_enc_hot_key_enabled is enabled. 2. Effective only if the IBM Security Access Manager for Enterprise Single Sign-On Hot Key is pressed when a user is not logged on to AccessAgent and computer is not locked. 3. If pid_lusm_sessions_max is greater than 1, AccessAgent with policy value 1 (Log off Windows) logs off the user from the desktop session and shows the computer locked screen. However, if the desktop is the default desktop, the setting in the policy pid_lusm_default_desktop_preserved_enabled determines whether the user can be logged off.
Registry	[D0] "EncHotKeyNotLoggedOnAction"
Type	DWORD Non-negative integer
Values	<ul style="list-style-type: none"> • #0: No action • #1: Log off Windows • #4: Lock computer • #9: Launch AccessAgent window (default value)
Scope	Machine System
Note	<ul style="list-style-type: none"> • Refreshed on sync for system policy. • Refreshed on use for machine policy.

Emergency Hot Key policies

Know the different emergency hot key policies and where to find and set these policies, their descriptions, and their default values.

Note: The Emergency hot key policies do not work in Windows 7 and later versions. If you enable the emergency hot key policies in client workstations running in these operating systems, the results might not be as expected because this scenario is not supported.



pid_emergency_hot_key_enabled

IMS Entry	Enable Emergency Hot Key?
Location	<ul style="list-style-type: none"> • AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Emergency Hot Key Policies • AccessAdmin > System > System policies > AccessAgent Policies > Emergency Hot Key Policies



pid_emergency_hot_key_enabled

Description	Whether the Emergency Hot Key is enabled. Note: <ol style="list-style-type: none">1. If the user presses this Hot Key at the computer locked screen, AccessAgent unlocks the computer without any credentials but logs off any logged on user from AccessAgent.2. To use the Emergency Hot Key, set the unlock option to 3.3. The use of the Emergency Hot Key is subject to proper behavior of auto-logoff from applications.4. This policy is not supported in Microsoft Windows Vista and later versions.
Registry	[D0] "EmergencyHotKeyEnabled"
Type	DWORD Boolean
Values	<ul style="list-style-type: none">• #1: Yes• #0: No (default value)• #True: Yes• #False: No (default value)
Scope	Machine System
Note	Refreshed on startup.



pid_emergency_hot_key_sequence

IMS Entry	Emergency Hot Key sequence
Location	<ul style="list-style-type: none">• AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Emergency Hot Key Policies• AccessAdmin > System > System policies > AccessAgent Policies > Emergency Hot Key Policies
Description	The Emergency Hot Key sequence. Maximum of 3 keys from the set: {Ctrl, Shift, Alt, Ins, Del, Home, End, PgUp, PgDn, Break, E}. Note: <ol style="list-style-type: none">1. Effective only if Emergency Hot Key is enabled.2. Modifying this policy requires a computer restart to implement the changes.3. This policy is not supported in Microsoft Windows 7 and later versions.
Registry	[D0] "EmergencyHotKeySequence"
Type	MULTI_SZ String list
Values	<ul style="list-style-type: none">• Ctrl• Alt• End
Scope	Machine System



pid_emergency_hot_key_sequence

Note	<ul style="list-style-type: none"> • Set a maximum of three key combinations: Ctrl, Shift, Alt, Ins, Del, Home, End, PgUp, PgDn, Break, E. • Use any of these 2 keys to minimize the probability of conflict with other applications: Ctrl, Shift, Alt. • Refreshed on startup.
-------------	--

Audit logging policies

Know the different audit logging policies and where to find and set these policies, their descriptions, and their default values.



pid_audit_log_by_aa_enabled

IMS Entry	Enable audit logging by AccessAgent?
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Audit Logging Policies
Description	Whether to enable audit logging by AccessAgent.
Registry	[D0] "AuditLogByAAEnabled"
Type	DWORD
Values	<ul style="list-style-type: none"> • #1: Yes (default value) • #0: No
Scope	Machine
Note	Refreshed on sync.

Background authentication policies

Know the different policies on background authentication, where to find and set these policies, their descriptions, and their default values.



pid_background_auth_option

IMS Entry	Option to perform background authentication
Location	AccessAdmin > Machine Policies > AccessAgent Policies > Logon/Logoff Policies
Description	Option to specify if AccessAgent can do an authentication with the IMS Server in the background.
Registry	
Type	Non-negative integer
Values	<ul style="list-style-type: none"> • #0: Never • #1: Only when the user logs on offline or performs fast unlock
Scope	Machine

 **pid_background_auth_option**

Note	<p>Important: If background authentication fails, the user is forcefully logged off from the workstation. If a Helpdesk officer is troubleshooting a user account and revokes the wallet accidentally, the user is logged off. In this case, the work of the user might be lost.</p> <ul style="list-style-type: none"> • When pid_fast_unlock_enabled is enabled, the user is authenticated after the desktop is opened. • When a user logs on offline, the user is still authenticated with the IMS Server when there is a connection between AccessAgent and the IMS Server.
-------------	--

 **pid_background_auth_retry_mins**

IMS Entry	Time interval in minutes to initiate background authentication
Location	AccessAdmin > Machine Policies > AccessAgent Policies > Logon/Logoff Policies
Description	Time interval, in minutes, to initiate background authentication if AccessAgent cannot connect to IMS Server
Registry	
Type	Non-negative integer
Values	<ul style="list-style-type: none"> • 0: Do not re-attempt background authentication • >0: Interval in minutes
Scope	Machine
Note	

Network policies

Know the different network-related policies, where to find and set these policies, their descriptions, and their default values.

 **pid_net_socket_timeout_secs**

IMS Entry	Timeout, in seconds, for making network socket connection
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > Network Policies
Description	Timeout, in seconds, for establishing a network connection with the IMS Server. This duration does not include the time used to send and receive messages.
Registry	
Type	
Values	1 (default value)
Scope	Machine
Note	Requires a machine restart.

 **pid_net_soap_timeout_secs**

IMS Entry	Timeout, in seconds, for making a SOAP call
Location	AccessAdmin > Machine Policy Templates > New template > Create new machine policy > AccessAgent Policies > Network Policies

 **pid_net_soap_timeout_secs**

Description	Timeout, in seconds, for sending or receiving a SOAP message.
Registry	
IMS Entry	
Type	
Values	60 (default value)
Scope	Machine
Note	Requires a machine restart.

Chapter 12. Policies for AccessAssistant

Use AccessAssistant policies to configure AccessAssistant and Web Workplace.

AccessAssistant is a Web-based interface that provides password self-help. Users can do AccessAgent tasks from web browsers by using Web Workplace. AccessAssistant contains automatic sign-on functions without installing AccessAgent on a computer.

For more information:

- “AccessAssistant and Web Workplace policies”

AccessAssistant and Web Workplace policies

Know the different AccessAssistant and Web Workplace policies for both user and system, where to find and set these policies, their descriptions, and their default values.



pid_accessanywhere_enabled

IMS Entry	Allow access to Wallet from AccessAssistant and Web Workplace?
Location	AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAssistant and Web Workplace Policies
Description	Whether the user is allowed to use AccessAssistant.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none">• #True: Yes (default value)• #False: No
Scope	User
Note	Refreshed on use.



pid_accessanywhere_second_factor_enabled

IMS Entry	Second factor authentication required for AccessAssistant and Web Workplace?
Location	AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAssistant and Web Workplace Policies
Description	Whether the user is required to authenticate by using a second factor in AccessAssistant.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none">• #True: Yes (default value)• #False: No
Scope	User
Note	Refreshed on use.



pid_accessanywhere_personal_app_enabled

IMS Entry	Display personal authentication services in AccessAssistant and Web Workplace?
Location	AccessAdmin > User Policy Templates > New template > Create new policy template > AccessAssistant and Web Workplace Policies
Description	Whether to display personal authentication services in AccessAssistant and Web Workplace. Note: 1. Effective only if pid_accessanywhere_enabled is True . 2. Some personal applications might not be displayed in AccessAssistant. These applications are not displayed because the Windows account (local computer) and some authentication services are not created by the Administrator, and can exist in the user scope only.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none"> • #True: Yes • #False: No (default value)
Scope	User
Note	Refreshed on sync.



pid_accessanywhere_app_sso_enabled

IMS Entry	Enable single sign-on to applications in AccessAssistant?
Location	AccessAdmin > System > System policies > AccessAssistant and Web Workplace Policies
Description	Whether the user can single sign-on to applications through AccessAssistant.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none"> • #True: Yes • #False: No (default value)
Scope	System
Note	Refreshed on sync.



pid_accessanywhere_edit_user_profile_enabled

IMS Entry	Enable editing of user profile in AccessAssistant and Web Workplace?
Location	AccessAdmin > System > System policies > AccessAssistant and Web Workplace Policies
Description	Whether the user profile can be edited by the user in AccessAssistant and Web Workplace.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none"> • #True: Yes • #False: No (default value)
Scope	System



pid_accessanywhere_edit_user_profile_enabled

Note	Refreshed on sync.
-------------	--------------------



pid_accessanywhere_sync_mins

IMS Entry	Interval, in minutes, for periodic synchronization of AccessAssistant and Web Workplace with the IMS Server?
Location	AccessAdmin > System > System policies > AccessAssistant and Web Workplace Policies
Description	Specifies the repeated interval at which AccessAssistant and Web Workplace synchronize policies and AccessProfiles with the IMS Server.
Registry	
Type	Positive integer
Values	
Scope	System
Note	



pid_accessanywhere_password_display_option

IMS Entry	Password display option in AccessAssistant
Location	AccessAdmin > System > System policies > AccessAssistant and Web Workplace Policies
Description	Option for the display of application passwords in AccessAssistant.
Registry	
Type	Non-negative integer
Values	<ul style="list-style-type: none"> • #0: Disable viewing of passwords • #1: Display password, no option to copy to clipboard • #2: Display password by default, with option to copy to clipboard (default) • #3: Copy to clipboard by default, with option to display password
Scope	System
Note	Refreshed on sync.



pid_accessanywhere_second_factor_default

IMS Entry	Default second authentication factor for AccessAssistant and Web Workplace
Location	AccessAdmin > System > System policies > AccessAssistant and Web Workplace Policies



pid_accessanywhere_second_factor_default

Description	The default second authentication factor for logging on to AccessAssistant and Web Workplace. Note: <ol style="list-style-type: none"> 1. Effective only if pid_accessanywhere_enabled and pid_accessanywhere_second_factor_enabled are True. 2. After entering the user name and password, AccessAssistant or Web Workplace will prompt for the default second factor. The user can still click the links to use other second factors. 3. If the default second factor is MAC, a MAC is automatically sent to the user after the user enters the user name and password. The MAC is sent through the preferred channel of the user. A message indicates where the MAC is sent, and sends links for the user to request for a MAC to be sent to another channel. 4. The user can change to a preferred MAC channel through the user profile settings page.
Registry	
Type	Positive integer
Values	<ul style="list-style-type: none"> • #1: Authorization code • #2: MAC • #3: OTP (timebased)
Scope	User
Note	Refreshed on use.



pid_unlock_account_enabled

IMS Entry	Enable unlocking of account by user in AccessAssistant and Web Workplace?
Location	AccessAdmin > System > System policies > AccessAssistant and Web Workplace Policies
Description	Whether the user account can be unlocked by the user in AccessAssistant and Web Workplace.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none"> • #True: Yes • #False: No (default value)
Scope	System
Note	Refreshed on sync.

Chapter 13. Policies for Applications and Authentication Services

In general, application-specific policies override authentication service-specific policies, which in turn, override general Wallet policies.

The Wallet inject password entry option default policy (`pid_wallet_inject_pwd_entry_option_default`) is used when the other two policies are not defined for a particular authentication service or application.

Some groups of policies have overlapping scopes. For example, policies with system scopes affect different ranges of entities.

- **Wallet inject password entry option default policy** (`pid_wallet_inject_pwd_entry_option_default`)
This policy defines the default password entry option for all authentication services and applications.
- **Authentication inject password entry option default policy** (`pid_auth_inject_pwd_entry_option_default`)
This policy defines the default password entry option for a specific authentication service.
- **Application inject password entry option default policy** (`pid_app_inject_pwd_entry_option_default`)
This policy defines the default password entry option for a specific application.

If the Authentication service inject password entry option default policy is defined for an authentication service, it overrides the Wallet inject password entry option default policy. The Wallet inject password entry option default policy is overridden when a default password entry option is needed for the authentication service.

Similarly, if the Application inject password entry option default policy is defined for a particular application, the application policy overrides the other two policies.

For more information:

- “Application policies”
- “Authentication service policies” on page 117

Application policies

Know the different application policies, where to find and set these policies, their descriptions, and their default values.



`pid_app_reauth_with_enc_pwd_enabled`

IMS Entry	Require re-authentication before single sign-on?
Location	AccessAdmin > System > Application policies > <Application name> > Application Policies
Description	Whether password re-authentication is required before single sign-on to the application. Note: Override authentication or authenticate again with a password.


pid_app_reauth_with_enc_pwd_enabled


Registry	
Type	Boolean
Values	<ul style="list-style-type: none"> • #True: Yes • #False: No (default value)
Scope	System
Note	Refreshed on sync.


pid_app_inject_pwd_entry_option_default

IMS Entry	Default single sign-on password entry option for the application
Location	AccessAdmin > System > Application policies > <Application name> > Application Policies
Description	Default single sign-on password entry option for the application. Note: This policy overrides the system-wide and the authentication service default single sign-on password entry options.
Registry	
Type	Positive integer
Values	<ul style="list-style-type: none"> • #1: Automatic log on • #2: Always (default value) • #3: Ask • #4: Never • #5: Certificate
Scope	System
Note	Refreshed on sync.


pid_app_wallet_logoff_action

IMS Entry	Action for the application, when user logs off AccessAgent
Location	AccessAdmin > System > Application policies > <Application name> > Application Policies
Description	Default action for the application when the user logs off from AccessAgent. This policy overrides the corresponding system-wide policy. The AccessProfile for the application must contain a logoff action, otherwise the application is not logged off. Note: <ol style="list-style-type: none"> 1. This policy overrides Wallet logoff action for applications default. 2. See the notes for Wallet logoff action for applications default. 3. For web applications, each URL is considered an application. Microsoft Internet Explorer is also considered an application. In this context, the web application policy overrides the Microsoft Internet Explorer policy, which overrides Wallet logoff action for applications default. 4. For Microsoft Internet Explorer and Windows Explorer, you can set the value to either 2 or 3. 5. This policy is set to 3 for Windows logon (application GINA) when the IMS Server is installed.

 pid_app_wallet_logoff_action

Registry	
Type	Positive integer
Values	<ul style="list-style-type: none"> • #1: Log off the application • #2: Close the application • #3: Do nothing (default value)
Scope	System
Note	Refreshed on use.

Authentication service policies

View the details of the different authentication service policies.

The different policies that you can configure for authentication service:

- “Password policies”
- “Authentication policies” on page 121

Password policies

Know the different authentication service password policies, where to find and set these policies, their descriptions, and their default values.

 pid_auth_fortification_random_pwd_enabled

IMS Entry	Enable manual password change with random password?
Location	AccessAdmin > User Policy Templates > New template > Create new policy template > Authentication Service Policies > <Authentication service name>
Description	Whether manual password change with a random password is enabled for the authentication service.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none"> • #True: Yes • #False: No (default value)
Scope	User
Note	Refreshed on sync.

 pid_auth_reauth_with_enc_pwd_enabled

IMS Entry	Require re-authentication before single sign-on?
Location	AccessAdmin > System > Authentication service policies > <Authentication service name> > Password Policies
Description	Whether password re-authentication is required before single sign-on for the authentication service. Note: Effective only if pid_auth_is_enterprise is enabled for the authentication service.
Registry	

 pid_auth_reauth_with_enc_pwd_enabled

Type	Boolean
Values	<ul style="list-style-type: none"> • #True: Yes • #False: No (default value)
Scope	System
Note	Refreshed on sync.

 pid_auth_pwd_is_ad_pwd

IMS Entry	Is the password the Windows logon password?
Location	AccessAdmin > System > Authentication service policies > <Authentication service name> > Password Policies
Description	Whether the authentication service is displayed as a Windows user account in AccessAdmin.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none"> • #True: Yes • #False: No (default value)
Scope	System
Note	Refreshed on use.

 pid_enc_pwd_min_length

IMS Entry	Minimum password length
Location	AccessAdmin > System > Authentication service policies > <Authentication service name> > Password Policies
Description	Minimum length of an acceptable password.
Registry	
Type	Non-negative integer
Values	6 (default value)
Scope	System
Note	<ul style="list-style-type: none"> • The value can range from 1 to 99. • Refreshed on sync.

 pid_enc_pwd_max_length

IMS Entry	Maximum password length
Location	AccessAdmin > System > Authentication service policies > <Authentication service name> > Password Policies
Description	Maximum length of an acceptable password.
Registry	
Type	Non-negative integer
Values	20 (default value)


pid_enc_pwd_max_length

Scope	System
Note	<ul style="list-style-type: none"> The value can range from 1 to 99. Refreshed on sync.


pid_enc_pwd_min_numerics_length

IMS Entry	Minimum number of numeric characters
Location	AccessAdmin > System > Authentication service policies > <Authentication service name> > Password Policies
Description	Minimum number of numeric characters for an acceptable password.
Registry	
Type	Non-negative integer
Values	0 (default value)
Scope	System
Note	<ul style="list-style-type: none"> The value can range from 0 to 99. Refreshed on sync.


pid_enc_pwd_min_alphabets_length

IMS Entry	Minimum number of alphabetic characters
Location	AccessAdmin > System > Authentication service policies > <Authentication service name> > Password Policies
Description	Minimum number of alphabetic characters for an acceptable password.
Registry	
Type	Non-negative integer
Values	0 (default value)
Scope	System
Note	<ul style="list-style-type: none"> The value can range from 0 to 99. Refreshed on sync.


pid_auth_fortification_pwd_min_special_characters_length

IMS Entry	Minimum number of special characters
Location	AccessAdmin > System > Authentication service policies > <Authentication service name> > Password Policies
Description	<p>Minimum number of special characters for an acceptable password for the authentication service.</p> <p>Note: Effective if pid_auth_fortification_random_pwd_enabled is enabled.</p>
Registry	
Type	Non-negative integer
Values	0 (default value)
Scope	System


pid_auth_fortification_pwd_min_special_characters_length

Note	<ul style="list-style-type: none"> • The value can range from 0 to 99. • Refreshed on sync.
-------------	---


pid_auth_fortification_pwd_max_numerics_length

IMS Entry	Maximum number of numeric characters
Location	AccessAdmin > System > Authentication service policies > <Authentication service name> > Password Policies
Description	Maximum number of numeric characters for an acceptable password for the authentication service. Note: Effective if pid_auth_fortification_random_pwd_enabled is enabled.
Registry	
Type	Non-negative integer
Values	10 (default value)
Scope	System
Note	<ul style="list-style-type: none"> • The value can range from 0 to 99. • Refreshed on sync.


pid_auth_fortification_pwd_max_alphabets_length

IMS Entry	Maximum number of alphabetic characters
Location	AccessAdmin > System > Authentication service policies > <Authentication service name> > Password Policies
Description	Maximum number of alphabetic characters for an acceptable password for the authentication service. Note: Effective if pid_auth_fortification_random_pwd_enabled is enabled.
Registry	
Type	Non-negative integer
Values	10 (default value)
Scope	System
Note	<ul style="list-style-type: none"> • The value can range from 0 to 99. • Refreshed on sync.


pid_auth_fortification_max_special_characters_length

IMS Entry	Maximum number of special characters
Location	AccessAdmin > System > Authentication service policies > <Authentication service name> > Password Policies
Description	Maximum number of special characters for an acceptable password for the authentication service. Note: Effective if pid_auth_fortification_random_pwd_enabled is enabled.
Registry	
Type	Non-negative integer


pid_auth_fortification_max_special_characters_length

Values	0 (default value)
Scope	System
Note	<ul style="list-style-type: none"> • The value can range from 0 to 99. • Set the value to 0 for no maximum limit. • Refreshed on sync.


pid_auth_fortification_pwd_mixed_case_enforced

IMS Entry	Enforce the use of both upper case and lower case characters?
Location	AccessAdmin > System > Authentication service policies > <Authentication service name> > Password Policies
Description	Whether to enforce both uppercase and lowercase characters for the password of the authentication service. Note: Effective if pid_auth_fortification_random_pwd_enabled is enabled.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none"> • #True: Yes • #False: No (default value)
Scope	System
Note	Refreshed on sync.

Authentication policies

Know the different authentication service authentication policies, where to find and set these policies, their descriptions, and their default values.


pid_auth_is_enterprise

IMS Entry	Is it an enterprise authentication service?
Location	AccessAdmin > System > Authentication service policies > <Authentication service name> > Authentication Policies
Description	Whether an authentication service is an enterprise authentication service.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none"> • #True: Yes • #False: No (default value)
Scope	System
Note	Refreshed on sync.


pid_auth_inject_pwd_entry_option_default

IMS Entry	Default single sign-on password entry option for the authentication service
Location	AccessAdmin > System > Authentication service policies > <Authentication service name> > Authentication Policies



pid_auth_inject_pwd_entry_option_default

Description	Default single sign-on password entry option for the authentication service. Note: 1. Effective only if pid_auth_is_enterprise is enabled for the authentication service. 2. Overrides Wallet inject password entry option default.
Registry	
Type	Positive integer
Values	<ul style="list-style-type: none"> • #1: Automatic log on • #2: Always (default value) • #3: Ask • #4: Never • #5: Certificate
Scope	System
Note	Refreshed on sync.



pid_auth_authentication_option

IMS Entry	Authentication modes to be supported
Location	AccessAdmin > System > Authentication service policies > <Authentication service name> > Authentication Policies
Description	Option to specify the supported authentication modes of AccessAgent for the authentication service. Note: Effective only if pid_auth_is_enterprise is enabled for the authentication service.
Registry	
Type	Positive integer
Values	<ul style="list-style-type: none"> • #1: Password (default value) • #2: SCR • #4: CAPI • #8: OTP (ISAM ESSO) • #16: MAC • #32 : CCOW • #: OTP (time-based) • #: OTP (OATH)
Scope	System
Note	<ul style="list-style-type: none"> • You can select multiple values. • Refreshed on sync.



pid_auth_capture_prompt_enabled

IMS Entry	Prompt user on auto-capture of password?
Location	AccessAdmin > System > Authentication service policies > <Authentication service name> > Authentication Policies



pid_auth_capture_prompt_enabled

Description	Whether the user must be prompted during auto-capture of password for the authentication service. Note: 1. Effective only if pid_auth_is_enterprise is enabled for the authentication service. 2. If the policy value is False , if a user is already logged on, and another user wants to use the same computer, the application passwords of the second user might be auto-captured into the Wallet of the first user. If pid_auth_capture_prompt_enabled is set to False for an authentication service, set pid_auth_account_max to 1 for the same authentication service.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none"> • #True: Yes (default value) • #False: No
Scope	System
Note	Refreshed on sync.



pid_auth_accounts_max

IMS Entry	Maximum number of accounts allowed for the authentication service
Location	<ul style="list-style-type: none"> • AccessAdmin > System > Authentication service policies > <Authentication service name> > Authentication Policies • AccessAdmin > User Policy Templates > New template > Create new policy template > Authentication Service Policies > <Authentication service name>
Description	Maximum number of accounts that a user can store for the authentication service. Note: 1. When the number of accounts reach or exceed the maximum that is specified by this policy: <ul style="list-style-type: none"> a. AccessAgent does not capture new accounts for this authentication service. b. If the user clicks Add new user in Wallet Manager, AccessAgent displays a prompt that the number of accounts reached the limit. 2. User policy, if defined, overrides system policy. 3. This policy is only applicable to AccessAgent.
Registry	Non-negative integer
Type	
Values	Unlimited (default value)
Scope	User System
Note	<ul style="list-style-type: none"> • The value can range from 0 to 10. • Refreshed on sync.

Chapter 14. Policies for ActiveCode

Use ActiveCode policies to configure how ActiveCodes are used in IBM Security Access Manager for Enterprise Single Sign-On.

ActiveCodes are randomly generated and event-based one-time passwords. The Mobile ActiveCode is generated on the IMS Server. The Mobile ActiveCode is delivered through a second channel, such as short message service (SMS) on mobile phones or through email.

For more information:

- “ActiveCode policies”

ActiveCode policies

Know the different ActiveCode policies, where to find and set these policies, their descriptions, and their default values. These policies apply only if ActiveCode support is configured on the IMS Server.

 **pid_mac_max_validity_count**

IMS Entry	Maximum number of Mobile ActiveCodes that may be valid for a user at any time.
Location	AccessAdmin > System > System policies > ActiveCode Policies
Description	Maximum number of valid Mobile ActiveCodes for a user at any time.
Registry	
Type	Positive integer
Values	3 (default value)
Scope	System
Note	<ul style="list-style-type: none">• The value can range from 1 to 7.• Refreshed on use.

 **pid_activecode_bypass_option**

IMS Entry	ActiveCode bypass option
Location	AccessAdmin > System > System policies > ActiveCode Policies
Description	Option for ActiveCode authentication bypass. Note: This option can be used for bypassing both Mobile ActiveCode and OTP ActiveCode (AccessAgent-OTP and on-board OTP).
Registry	
Type	Non-negative integer
Values	<ul style="list-style-type: none">• #1: Authorization code and password• #2: Authorization code and enterprise account password• #4: Authorization code and secret
Scope	System
Note	Refreshed on use.


pid_activecode_append_secret_option

IMS Entry	Option for appending a secret to Mobile ActiveCode
Location	AccessAdmin > System > System policies > ActiveCode Policies
Description	Option for appending a secret to Mobile ActiveCode. Note: The order is also specified in the policy values.
Registry	
Type	Non-negative integer
Values	<ul style="list-style-type: none"> • #0: MAC only (no appending of secret) (default value) • #1: MAC + password • #2: MAC + Enterprise account password • #3: MAC + Administrator- assigned secret • #4: Password + MAC • #5: Enterprise account password + MAC • #6: Administrator-assigned secret + MAC
Scope	System
Note	Refreshed on use.


pid_otp_append_secret_option

IMS Entry	Option for appending a secret to OTP (time-based) and OTP (OATH)
Location	AccessAdmin > System > System policies > ActiveCode Policies
Description	Option for appending a secret to OTP (time-based) and OTP (OATH). Note: <ol style="list-style-type: none"> 1. Not applicable to AA-OTP. 2. The order is also specified in the policy values.
Registry	
Type	Non-negative integer
Values	<ul style="list-style-type: none"> • #0: OTP only (no appending of secret) (default value) • #1: OTP + password • #2: OTP + Enterprise account password • #3: OTP + Administrator- assigned secret • #4: Password + OTP • #5: Enterprise account password + OTP • #6: Administrator-assigned secret + OTP
Scope	System
Note	Refreshed on use.


pid_activecode_admin_assigned_secret_name

IMS Entry	Identity attribute name of the Administrator-assigned secret
Location	AccessAdmin > System > System policies > ActiveCode Policies



pid_activecode_admin_assigned_secret_name

Description	Identity attribute name of the Administrator-assigned secret, for appending to ActiveCode. Note: <ol style="list-style-type: none">1. This can be used for both Mobile ActiveCode and OTP ActiveCode (AccessAgent-OTP and on-board OTP).2. Effective only if ActiveCode append secret option is 3.
Registry	
Type	String
Values	
Scope	System
Note	Refreshed on use.



pid_otp_reset_sample_count

IMS Entry	Number of consecutive OTPs needed for resetting an OTP (OATH) token
Location	AccessAdmin > System > System policies > ActiveCode Policies
Description	Number of consecutive OTPs to be obtained from a user for resetting an OTP (OATH) token.
Registry	
Type	Positive integer
Values	3 (default value)
Scope	System
Note	<ul style="list-style-type: none">• The value can range from 1 to 5.• Refreshed on use.

Chapter 15. Policies for Privileged Identity Management

Use privileged identity management policies to configure how the policies are administered when IBM Security Privileged Identity Manager is deployed.

Use privileged identity management policies to configure the authentication service, check-in and check-out options, IBM Security Identity Manager host name, and session recording options.

IBM Security Privileged Identity Manager configuration policies

Know the privileged identity management policies, where to find the policies, their descriptions, and their default values. These policies apply only if the IBM Security Privileged Identity Manager solution is installed.

 **pid_pim_cico_svc_url**

IMS Entry	IBM Security Identity Manager URL
Location	AccessAdmin > System > System policies > IBM Security Privileged Identity Manager Configuration Policies
Description	Service URL for IBM Security Identity Manager shared access service. For example: <code>https://<isim_host>/itim/services/WSSharedAccessService</code>
Registry	
Type	String
Values	
Scope	System
Note	Refreshed on sync.

 **pid_pim_itim_auth_svc_id**

IMS Entry	IBM Security Identity Manager Authentication Service ID
Location	AccessAdmin > System > System policies > IBM Security Privileged Identity Manager Configuration Policies
Description	Authentication service ID for identifying the IBM Security Identity Manager credential that is stored in the user's wallet.
Registry	
Type	String
Values	
Scope	System
Note	Refreshed on sync.

 **pid_recorder_server**

IMS Entry	Privileged Session Recorder Server URL
Location	AccessAdmin > System > System policies > IBM Security Privileged Identity Manager Configuration Policies


pid_recorder_server

Description	URL of the Privileged Session Recorder Server. For example: https://psr.example.com/recorder/collector
Registry	
Type	
Values	String
Scope	System
Note	Refreshed on sync.


pid_recorder_image_capture_option

IMS Entry	Privileged Session Recorder image capture option
Location	AccessAdmin > System > System policies > IBM Security Privileged Identity Manager Configuration Policies
Description	Color depth of the images to capture for session recording.
Registry	
Type	Non-negative integer
Values	<ul style="list-style-type: none"> • #0: Full Color • #1: Grayscale (default value)
Scope	System
Note	Refreshed on sync.


pid_recorder_keyboard_capture_option

IMS Entry	Privileged Session Recorder keyboard capture option
Location	AccessAdmin > System > System policies > IBM Security Privileged Identity Manager Configuration Policies
Description	Specifies keyboard events to capture during a screen-based session recording.
Registry	
Type	Non-negative integer
Values	<ul style="list-style-type: none"> • #0: Log all key inputs (default value) • #1: Log only special keys • #2: Do not log any key inputs
Scope	System
Note	Refreshed on sync. This option does not apply to text-based recordings.


pid_recorder_enabled

IMS Entry	Enable Session Recording?
Location	AccessAdmin > System > System policies > IBM Security Privileged Identity Manager Configuration Policies


pid_recorder_enabled

Description	Whether to record sessions created using shared access identities.
Registry	
Type	Boolean
Values	<ul style="list-style-type: none"> • No (default) • Yes
Scope	System
Note	Refreshed on sync.


pid_collector_comm_fail_action

IMS Entry	Action that the client computer takes when Privileged Session Recorder server communication fails
Location	AccessAdmin > System > System policies > IBM Security Privileged Identity Manager Configuration Policies
Description	Specifies the action to take on the client computer when the Privileged Session Recorder Server is not reachable after a maximum number of retries.
Registry	
Type	Non-negative integer
Values	<ul style="list-style-type: none"> • #0: Take no action. • #1: Block user inputs. • #2: Close application.
Scope	System
Note	Refreshed on sync.


pid_collector_comm_fail_limit

IMS Entry	Number of connection retries to the Privileged Session Recorder server
Location	AccessAdmin > System > System policies > IBM Security Privileged Identity Manager Configuration Policies
Description	Specifies the maximum number of connection attempts before determining that the Privileged Session Recorder Server is not reachable.
Registry	
Type	Non-negative integer
Values	3 (default value)
Scope	System
Note	Refreshed on sync.


pid_collector_comm_fail_retry_interval

IMS Entry	Time interval between connection retries to the Privileged Session Recorder Server
Location	AccessAdmin > System > System policies > IBM Security Privileged Identity Manager Configuration Policies



pid_collector_comm_fail_retry_interval

Description	Time interval, in seconds, between attempts to connect to the Privileged Session Recorder Server.
Registry	
Type	Non-negative integer
Values	15 (default value)
Scope	System
Note	Refreshed on sync.

Chapter 16. Other policies

Know other policies, where to find and set these policies, their descriptions, and their default values.

Location	Registry Editor > HKEY_LOCAL_MACHINE > SOFTWARE > IBM > ISAM ESSO > DeploymentOptions
Description	Controls the Help link on the AccessAgent user interface.
Registry	[D0] "AAOnlineHelpLink"
Type	REG_SZ
Values	http://www.ibm.com/support/knowledgecenter/SS9JLE_8.2.1 (default value)
Scope	
Note	Set this policy to empty to remove the Help link from the AccessAgent user interface. To specify another URL for the Help link, you can replace the default value with another URL.

Location	Registry Editor > HKEY_LOCAL_MACHINE > SOFTWARE > IBM > ISAM ESSO > ECSS > DeploymentOptions
Description	Controls the Help link on the Observer window.
Registry	[D0] "ObsOnlineHelpEnabled"
Type	DWORD
Values	<ul style="list-style-type: none"> • #0: Disables the Help button (default value) • #1: Enables the Help button
Scope	
Note	

Location	Registry Editor > HKEY_LOCAL_MACHINE > SOFTWARE > IBM > ISAM ESSO > DeploymentOptions
Description	
Registry	[D0] "WindowsEventLogEnabled"
Type	DWORD
Values	<ul style="list-style-type: none"> • #0: Disables event reporting in the Windows Event log (default value) • #1: Enables event reporting in the Windows Event log
Scope	
Note	

Location	Registry Editor > HKEY_LOCAL_MACHINE > SOFTWARE > IBM > ISAM ESSO > DeploymentOptions
Description	

Registry	[D0] "SystemModalMessageEnabled"
Type	DWORD
Values	<ul style="list-style-type: none"> • #0: Disables the System Modal message box (default value) • #1: Enables the System Modal message box
Scope	
Note	

Location	Registry Editor > HKEY_LOCAL_MACHINE > SOFTWARE > IBM > ISAM ESSO > DeploymentOptions
Description	
Registry	[D0] "UIDirectionLToR"
Type	DWORD
Values	<ul style="list-style-type: none"> • #0: False • #1: True (default value)
Scope	
Note	

Chapter 17. Policy limitations in Windows 7

There are some policies that do not work in Windows 7.

- **pid_unlock_option**

The option **Only the same user can unlock, but different user can re-log on to Windows** does not work in Windows 7.

- **pid_rfid_tap_different_action**

Option	Action in Windows XP	Action in Windows 7
No action	Works as expected	Works as expected
Lock computer	Works as expected	Works as expected
Log off Wallet and lock computer	Works as expected	Works as expected
Switch user	Switches to another user in the desktop	Switches to another user in the desktop. Fast user switching takes place if <code>pid_fast_user_switching_enabled</code> is enabled. In this scenario, the user is switched to a different session.
Log off Windows and log on as new user	Works as expected	Does not work

- **pid_fingerprint_tap_different_action**

Option	Action in Windows XP	Action in Windows 7
No action	Works as expected	Works as expected
Lock computer	Works as expected	Works as expected
Log off Wallet and lock computer	Works as expected	Works as expected
Switch user	Switches to another user in the desktop	Switches to another user in the desktop. Fast user switching takes place if <code>pid_fast_user_switching_enabled</code> is enabled. In this scenario, the user is switched to a different session.
Log off Windows and log on as new user	Works as expected	Does not work

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law :

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to

IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com[®] are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and trademark information; at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.



Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Privacy Policy Considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering uses other technologies that collect each user's user name, password or other personally identifiable information for purposes of session management, authentication, single sign-on configuration or other usage tracking or functional purposes. These technologies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at <http://www.ibm.com/privacy> and IBM’s Online Privacy Statement at <http://www.ibm.com/privacy/details/us/en> sections entitled “Cookies, Web Beacons and Other Technologies” and “Software Products and Software-as-a Service”.

Glossary

This glossary includes terms and definitions for IBM Security Access Manager for Enterprise Single Sign-On.

The following cross-references are used in this glossary:

- See refers you from a term to a preferred synonym, or from an acronym or abbreviation to the defined full form.
- See also refers you to a related or contrasting term.

To view glossaries for other IBM products, go to www.ibm.com/software/globalization/terminology (opens in new window).

A

account data

The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag

A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item

The user credentials required for logon.

account data item template

A template that defines the properties of an account data item.

account data template

A template that defines the format of account data to be stored for credentials captured using a specific AccessProfile.

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)

A hierarchical directory service that enables centralized, secure management

of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential

The Active Directory user name and password.

Active Directory password synchronization

An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification (active RFID)

A second authentication factor and presence detector. See also radio frequency identification.

active RFID

See active radio frequency identification.

AD See Active Directory.

administrator

A person responsible for administrative tasks such as access authorization and content management. Administrators can also grant levels of authority to users.

API See application programming interface.

application

A system that provides the user interface for reading or entering the authentication credentials.

application policy

A collection of policies and attributes governing access to applications.

application programming interface (API)

An interface that allows an application program that is written in a high-level language to use specific data or functions of the operating system or another program.

audit A process that logs the user, Administrator, and Helpdesk activities.

authentication factor

The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication

factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service

A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization code

An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

auto-capture

A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on

A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

B**base distinguished name**

A name that indicates the starting point for searches in the directory server.

base image

A template for a virtual desktop.

bidirectional language

A language that uses a script, such as Arabic and Hebrew, whose general flow of text proceeds horizontally from right to left, but numbers, English, and other left-to-right language text are written from left to right.

bind distinguished name

A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory.

biometrics

The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

C

CA See certificate authority.

CAPI See cryptographic application programming interface.

Card Serial Number (CSN)

A unique data item that identifies a hybrid smart card. It has no relation to the certificates installed in the smart card

CCOW

See Clinical Context Object Workgroup.

cell

A group of managed processes that are federated to the same deployment manager and can include high-availability core groups.

certificate

In computer security, a digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)

A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate.

CLI See command-line interface.

Clinical Context Object Workgroup (CCOW)

A vendor independent standard, for the interchange of information between clinical applications in the healthcare industry.

cluster

A group of application servers that collaborate for the purposes of workload balancing and failover.

command-line interface (CLI)

A computer interface in which the input and output are text based.

credential

Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a

user ID and password are credentials that allow access to network and system resources.

cryptographic application programming interface (CAPI)

An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

cryptographic service provider (CSP)

A feature of the i5/OS™ operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

CSN See Card Serial Number.

CSP See cryptographic service provider.

D

dashboard

An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

database server

A software program that uses a database manager to provide database services to other software programs or computers.

data source

The means by which an application accesses data from a database.

deployment manager

A server that manages and configures operations for a logical group or cell of other servers.

deployment manager profile

A WebSphere Application Server runtime environment that manages operations for a logical group, or cell, of other servers.

deprovision

To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool

A collection of virtual desktops of similar

configuration intended to be used by a designated group of users.

directory

A file that contains the names and controlling information for objects or other directories.

directory service

A directory of names, profile information, and machine addresses of every user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery

The process of restoring a database, system, policies after a partial or complete site failure that was caused by a catastrophic event such as an earthquake or fire. Typically, disaster recovery requires a full backup at another location.

disaster recovery site

A secondary location for the production environment in case of a disaster.

distinguished name (DN)

The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region.

DLL See dynamic link library.

DN See distinguished name.

DNS See domain name server.

domain name server (DNS)

A server program that supplies name-to-address conversion by mapping domain names to IP addresses.

dynamic link library (DLL)

A file containing executable code and data bound to a program at load time or run time, rather than during linking. The code and data in a DLL can be shared by several applications simultaneously.

E

enterprise directory

A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)

A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

ESSO See enterprise single sign-on.

event code

A code that represents a specific event that is tracked and logged into the audit log tables.

F

failover

An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

fast user switching

A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)

A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

FIPS See Federal Information Processing Standard.

fix pack

A cumulative collection of fixes that is released between scheduled refresh packs, manufacturing refreshes, or releases. A fix pack updates the system to a specific maintenance level.

FQDN

See fully qualified domain name.

fully qualified domain name (FQDN)

In Internet communications, the name of a host system that includes all of the subnames of the domain name. An example of a fully qualified domain name is rchland.vnet.ibm.com. See also host name.

G

GINA See graphical identification and authentication.

GPO See group policy object.

graphical identification and authentication (GINA)

A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)

A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

high availability (HA)

The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

host name

In Internet communication, the name given to a computer. The host name might be a fully qualified domain name such as mycomputer.city.company.com, or it might be a specific subname such as mycomputer. See also fully qualified domain name, IP address.

hot key

A key sequence used to shift operations

between different applications or between different functions of an application.

hybrid smart card

An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

interactive graphical mode

A series of panels that prompts for information to complete the installation.

IP address

A unique address for a device or logical unit on a network that uses the Internet Protocol standard. See also host name.

J

Java Management Extensions (JMX)

A means of doing management of and through Java technology. JMX is a universal, open extension of the Java programming language for management that can be deployed across all industries, wherever management is needed.

Java runtime environment (JRE)

A subset of a Java developer kit that contains the core executable programs and files that constitute the standard Java platform. The JRE includes the Java virtual machine (JVM), core classes, and supporting files.

Java virtual machine (JVM)

A software implementation of a processor that runs compiled Java code (applets and applications).

JMX See Java Management Extensions.

JRE See Java runtime environment.

JVM See Java virtual machine.

K

keystore

In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication

and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

Lightweight Directory Access Protocol (LDAP)

An open protocol that uses TCP/IP to provide access to directories that support an X.500 model. An LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode

A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Terminal or Citrix Server and improves the single sign-on startup duration.

linked clone

A copy of a virtual machine that shares virtual disks with the parent virtual machine in an ongoing manner.

load balancing

The monitoring of application servers and management of the workload on servers. If one server exceeds its workload, requests are forwarded to another server with more capacity.

lookup user

A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

managed node

A node that is federated to a deployment manager and contains a node agent and can contain managed servers. See also node.

mobile authentication

An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

N

network deployment

The deployment of an IMS™ Server on a WebSphere Application Server cluster.

node A logical group of managed servers. See also managed node.

node agent

An administrative agent that manages all application servers on a node and represents the node in the management cell.

O

one-time password (OTP)

A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

OTP See one-time password.

OTP token

A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

P

password aging

A security feature by which the superuser can specify how often users must change their passwords.

password complexity policy

A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

personal identification number (PIN)

In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

PIN See personal identification number.

pinnable state

A state from an AccessProfile widget that

can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

policy template

A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector

A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor

The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

private key

In computer security, the secret half of a cryptographic key pair that is used with a public key algorithm. The private key is known only to its owner. Private keys are typically used to digitally sign data and to decrypt data that has been encrypted with the corresponding public key.

provision

To provide, deploy, and track a service, component, application, or resource. See also deprovision.

provisioning API

An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge

An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning system

A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

Public Key Cryptography Standards (PKCS)

A set of industry-standard protocols used for secure information exchange on the Internet. Domino® Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

published application

An application installed on Citrix XenApp server that can be accessed from Citrix ICA Clients.

published desktop

A Citrix XenApp feature where users have remote access to a full Windows desktop from any device, anywhere, at any time.

R**radio frequency identification (RFID)**

An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS

See remote authentication dial-in user service.

random password

An arbitrarily generated password used to increase authentication security between clients and servers.

RDP See remote desktop protocol.

registry

A repository that contains access and configuration information for users, systems, and software.

registry hive

In Windows systems, the structure of the data stored in the registry.

remote authentication dial-in user service (RADIUS)

An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

remote desktop protocol (RDP)

A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP

supports different network topologies and multiple connections.

replication

The process of maintaining a defined set of data in more than one location. Replication involves copying designated changes for one location (a source) to another (a target) and synchronizing the data in both locations.

revoke

To remove a privilege or an authority from an authorization identifier.

RFID See radio frequency identification.

root CA

See root certificate authority.

root certificate authority (root CA)

The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

S

scope A reference to the applicability of a policy, at the system, user, or machine level.

secret question

A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access

The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Sockets Layer (SSL)

A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

Secure Sockets Layer virtual private network (SSL VPN)

A form of VPN that can be used with a standard web browser.

Security Token Service (STS)

A web service that is used for issuing and exchanging security tokens.

security trust service chain

A group of module instances that are

configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

serial ID service provider interface

A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number

A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator

A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)

An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use the device as a second factor in AccessAgent.

signature

In profiling, unique identification information for any application, window, or field.

sign-on automation

A technology that works with application user interfaces to automate the sign-on process for users.

sign up

To request a resource.

silent mode

A method for installing or uninstalling a product component from the command line with no GUI display. When using silent mode, you specify the data required by the installation or uninstallation program directly on the command line or in a file (called an option file or response file).

Simple Mail Transfer Protocol (SMTP)

An Internet application protocol for transferring mail among users of the Internet.

single sign-on (SSO)

An authentication process in which a user can access more than one system or application by entering a single user ID and password.

smart card

An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

smart card middleware

Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot

A captured state, data, and hardware configuration of a running virtual machine.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet. See also web service.

SPI See service provider interface.

SSL See Secure Sockets Layer.

SSL VPN

See Secure Sockets Layer virtual private network.

SSO See single sign-on.

stand-alone deployment

A deployment where the IMS Server is deployed on an independent WebSphere Application Server profile.

stand-alone server

A fully operational server that is managed independently of all other servers, using its own administrative console.

strong authentication

A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity

An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

STS See Security Token Service.

system modal message

A system dialog box that is typically used to display important messages. When a system modal message is displayed, nothing else can be selected on the screen until the message is closed.

T**terminal emulator**

A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

terminal type (tty)

A generic device driver for a text display. A tty typically performs input and output on a character-by-character basis.

thin client

A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

transparent screen lock

An feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

trigger

In profiling, an event that causes transitions between states in a states engine, such as, the loading of a web page or the appearance of a window on the desktop.

trust service chain

A chain of modules that operate in different modes such as validate, map, and issue truststore.

truststore

In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for authentication purposes in web transactions. In some applications, these trusted certificates are

moved into the application keystore to be stored with the private keys. See also keystore.

tty See terminal type.

two-factor authentication

The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U**uniform resource identifier**

A compact string of characters for identifying an abstract or physical resource.

user credential

Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning

The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user provisioning

The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

VB See Visual Basic.

virtual appliance

A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual channel connector

A connector that is used in a terminal services environment. The virtual channel connector establishes a virtual communication channel to manage the remote sessions between the Client AccessAgent component and the Server AccessAgent.

virtual desktop

A user interface in a virtualized environment, stored on a remote server.

virtual desktop infrastructure

An infrastructure that consists of desktop operating systems hosted within virtual machines on a centralized server.

Virtual Member Manager (VMM)

A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)

An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure.

Visual Basic (VB)

An event-driven programming language and integrated development environment (IDE) from Microsoft.

VMM See Virtual Member Manager.

VPN See virtual private network.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching

The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager

The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web server

A software program that is capable of servicing Hypertext Transfer Protocol (HTTP) requests.

web service

A self-contained, self-describing modular application that can be published, discovered, and invoked over a network using standard network protocols. Typically, XML is used to tag the data, SOAP is used to transfer the data, WSDL is used for describing the services available, and UDDI is used for listing what services are available. See also SOAP.

WS-Trust

A web services security specification that defines a framework for trust models to establish trust between web services.

Index

A

- AccessAgent policies 49
 - behavior 56, 115
 - user interface 56
- AccessAssistant and Web Workplace
 - policies 111
 - about 111
 - configurable text 35
 - usage settings for AccessAssistant and Web Workplace 111
- accessibility viii
- accessibility policies 35
- ActiveCode policies 125
- audit logging policies 45, 107
- audit settings 45
- authentication factor policies 7
- authentication policies 7
- authentication services policies 115, 117, 121

B

- background authentication policies 107
- bidirectional support policy 133

C

- change password 9
- Citrix Server policies 43
- customize text 21

D

- desktop inactivity policies 63
- display policies 57

E

- education viii
- emergency hot key policies 105
- ESSO Credential Provider policies
 - configurable text 21
- ESSO GINA policies
 - behavior 59
 - configurable text 21

F

- fingerprint authentication policies 85

G

- glossary 141

H

- hot key policies 102
- hybrid smart card authentication
 - policies 75

I

- IBM
 - Software Support viii
 - Support Assistant viii

L

- lightweight mode policies 43
- lock/unlock policies 66
- log file policies 47
- log on/log off policies 95
- log policies 45

N

- network policies 45, 108

O

- online
 - publications v
 - terminology v
- online help policy 133

P

- password aging policies 9
- password change policies 11
- password policies 117
- password strength policies 9, 12
- policies 129
 - about 1
 - accessibility 35
 - ActiveCode 125
 - application 115
 - audit logging 107
 - authentication 7, 121
 - authentication service 117
 - background authentication 107
 - desktop inactivity 63
 - emergency hot key 105
 - ESSO GINA 59
 - fingerprint 85
 - hot key 102
 - hybrid smart card 75
 - legends 3
 - lightweight mode 43
 - lock/unlock 66
 - log on/log off 95
 - logs 47
 - network 108
 - password 117

policies (*continued*)

- password aging 9
- password change 11
- password strength 12
- registry 133
- RFID 79
- roaming session 94
- self-service password reset 15
- self-service registration 16
- set priorities 5
- shared desktop 37
- sign up 17
- smart card 74
- symbols 3
- temporary file 47
- Terminal Server 88
- troubleshooting 45
- view priorities 5
- Wallet 49
- window display 57
- policy limitations 135
- private desktop policies 37
- Privileged Identity Management
 - policies 129
- problem-determination viii
- publications
 - accessing online v
 - list of for this product v
 - statement of good security practices ix

R

- registry policies 133
- RFID policies 79
- roaming session policies 94

S

- second factor bypass 16
- self-service password reset policies 15
- self-service registration policies 16
- session recording policies 129
- shared desktop policies 37
- sign up policies 15
 - configurable text 34
 - customize 17
- smart card authentication policies 74
- system modal message policy 133

T

- temporary file policies 45, 47
- Terminal Server policies 43, 88
- text policies
 - AccessAssistant and Web Workplace 35
 - ESSO Credential Provider 21
 - ESSO GINA 21
 - sign up 34

text policies (*continued*)
 unlock 25
 user interface 21
training viii
troubleshooting policies 45

U

unlock text policies 25
user interface 21, 56

W

Wallet policies 49
Windows 7 limitations 135
windows event log policy 133



Printed in USA

SC23-9694-04

