IBM® Security Access Manager for Enterprise Single Sign-On
Version 8.2

Policies Definition Guide

SC23-9694-01

IBM® Security Access Manager for Enterprise Single Sign-On
Version 8.2

Policies Definition Guide

SC23-9694-01

Note
Before using this information and the product it supports, read the information in "Notices" on page 143.

Edition notice

Note: This edition applies to version 8.2 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.

Contents

About this publication

The IBM® Security Access Manager for Enterprise Single Sign-On provides sign-on and sign-off automation, authentication management, and user tracking to provide a seamless path to strong digital identity. The *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide* provides information about the policies that can be set for the product. The policies can be set by using either AccessAdmin or by updating registry entries.

Intended audience

This publication is for technical users who understand how IBM Security Access Manager for Enterprise Single Sign-On can be enhanced and customized for a specific use for the customer.

This publication is for Administrators and system programmers who must perform the following tasks:

- Use policies to enable settings for IBM Security Access Manager for Enterprise Single Sign-On
- Set and maintain policies

Readers must be familiar with the following topics:

- Using AccessAdmin or modifying registry entries
- Information specific to the organization. For example: types of applications used by the organization and authentication factors.

What this publication contains

This publication contains the following sections:

- Chapter 1, "Policies in AccessAdmin," on page 1

  Provides an overview of the different scopes and dependencies of policies.
- Chapter 2, "Policy legends," on page 3

  Provides an overview of legends and symbols used for the policies in this guide.
- Chapter 3, "Viewing and setting policy priorities," on page 5

  Provides an overview of how to view and set policy priorities in this guide.
- Chapter 4, "Policies for Authentication Factors," on page 7

  Describes the different authentication policies such as Wallet and second authentication factors.
- Chapter 5, "Policies for Password Management," on page 9

  Contains information about policies about password aging, enabling password change, and password strength.
- Chapter 6, "Policies for Sign up and Password Reset," on page 15

  Contains information about policies on setting secret questions and answers, registering additional secrets during sign-up, and using a second authentication factor during sign-up.
- Chapter 7, "Policies for Configurable Text and Accessibility," on page 25

  Contains information about the policies for the messages displayed for EnGINA, computer unlock, RFID, and so on.

- Chapter 8, “Policies for Private and Shared desktops,” on page 43

  Contains information about the policies in a shared workstation session.
- Chapter 9, “Policies for Terminal Server/Citrix,” on page 49

  Contains information about enabling the lightweight mode that enhances performance by using less memory footprint.
- Chapter 10, “Policies for Debugging Management and Control,” on page 51

  Contains information about the policies for auditing, troubleshooting, memory reduction, and logs.
- Chapter 11, “Policies for Wallet and AccessAgent,” on page 57

  Contains information about the Wallet policies, such as enabling the caching of Wallets, the maximum number of cached Wallets, and Wallet synchronization settings. This section also contains information about AccessAgent policies, such as EnGINA settings, second authentication factor settings, logon policies, Terminal Server policies, and so on.
- Chapter 12, “Policies for AccessAssistant,” on page 121

  Contains information about the policies for AccessAssistant and Web Workplace.
- Chapter 13, “Policies for Applications and Authentication Services,” on page 125

  Contains information about the policies for applications used by your organization. This section also contains information about the Wallet policies, such as enabling the caching of Wallets, the maximum number of cached Wallets, and Wallet synchronization settings.
- Chapter 14, “Policies for ActiveCode,” on page 135

  Contains information about the policies for Mobile ActiveCode.
- Chapter 15, “Other policies,” on page 139

  Contains policies that configure the Help, and system modal messages.
- “Policy limitations in Windows 7,” on page 141

  Contains information about private desktop policies that are not supported on Windows Vista and Windows 7.

Publications

This section lists publications in the IBM Security Access Manager for Enterprise Single Sign-On library. The section also describes how to access Tivoli® publications online and how to order Tivoli publications.

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*, CF38DML

  Read this guide for 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*, SC23995203

  Read this guide before you do any installation or configuration tasks. This guide helps you to plan your deployment and prepare 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.

- *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*, GI11930901

  Read this guide for the 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, and also do the initial configurations 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*, GC23969201

  Read this guide if you want to configure the IMS Server settings, the AccessAgent user interface, and its behavior.
- *IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide*, SC23995103

  This guide is intended for the Administrators. It covers the different Administrator tasks. This 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 Help Desk Guide*, SC23995303

  This guide is intended for Help desk officers. The guide helps Help desk officers to manage 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 Policies Definition Guide*, SC23969401

  Read this guide for the 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 Troubleshooting and Support Guide*, GC23969301

  Read this guide if you have any 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 AccessStudio Guide*, SC23995603

  Read this guide if you want to create or edit profiles. 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 Provisioning Integration Guide*, SC23995703

  Read this guide for 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*, SC14764600

Read this guide if you want to install and configure the Web API for credential management.

- *IBM Security Access Manager for Enterprise Single Sign-On Lightweight AccessAgent mode on Terminal Server SDK Guide*, SC14765700

  Read this guide for the details on how to develop a virtual channel connector that integrates AccessAgent with Terminal Services applications.

- *IBM Security Access Manager for Enterprise Single Sign-On Serial ID SPI Guide*, SC14762600

  IBM Security Access Manager for Enterprise Single Sign-On has a Service Provider Interface (SPI) for devices that contain serial numbers, such as RFID. See this guide to know 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 Context Management Integration Guide*, SC23995403

  Read this guide if you want to install and configure the Context Management solution.

- *IBM Security Access Manager for Enterprise Single Sign-On User Guide*, SC23995003

  This guide is intended for the end users. This guide provides instructions for using AccessAgent and Web Workplace.

- *IBM Security Access Manager for Enterprise Single Sign-On Error Message Reference Guide*, GC14762400

  This guide describes all the informational, warning, and error messages associated with IBM Security Access Manager for Enterprise Single Sign-On.

Accessing terminology online

The IBM Terminology Web site consolidates the terminology from IBM product libraries in one convenient location. You can access the Terminology Web site at the following Web address:

http://www.ibm.com/software/globalization/terminology

Accessing publications online

IBM posts publications for this and all other Tivoli products, as they become available and whenever they are updated, to the Tivoli Information Center Web site at http://www.ibm.com/tivoli/documentation.

Note: If you print PDF documents on other than letter-sized paper, set the option in the **File** > **Print** window that allows Adobe Reader to print letter-sized pages on your local paper.

Ordering publications

You can order many Tivoli publications online at http://www.elink.ibmlink.ibm.com/publications/servlet/pbi.wss.

You can also order by telephone by calling one of these numbers:

- In the United States: 800-879-2755
- In Canada: 800-426-4968

In other countries, contact your software account representative to order Tivoli publications. To locate the telephone number of your local representative, perform the following steps:

1. Go to http://www.elink.ibmlink.ibm.com/publications/servlet/pbi.wss.
2. Select your country from the list and click **Go**.
3. Click **About this site** in the main panel to see an information page that includes the telephone number of your local representative.

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*.

Tivoli technical training

For Tivoli technical training information, see the following IBM Tivoli Education Web site at http://www.ibm.com/software/tivoli/education.

Tivoli user groups

Tivoli user groups are independent, user-run membership organizations that provide Tivoli users with information to assist them in the implementation of Tivoli Software solutions. Through these groups, members can share information and learn from the knowledge and experience of other Tivoli users. Tivoli user groups include the following members and groups:

- 23,000+ members
- 144+ groups

Access the link for the Tivoli Users Group at www.tivoli-ug.org.

Support information

If you have a problem with your IBM software, you want to resolve it quickly. IBM provides the following ways for you to obtain the support you need:

Online
Go to the IBM Software Support site at http://www.ibm.com/software/support/probsub.html and follow the instructions.

IBM Support Assistant
The IBM Support Assistant is a free local software serviceability workbench that helps you resolve questions and problems with IBM software products. The IBM Support Assistant provides quick access to support-related information and serviceability tools for problem determination. To install the IBM Support Assistant software, go to http://www.ibm.com/software/support/isa.

Troubleshooting Guide
For more information about resolving problems, see the *IBM Security Access Manager for Enterprise Single Sign-On Troubleshooting and Support Guide*.

Conventions used in this publication

This publication uses several conventions for special terms and actions, operating system-dependent commands and paths, and margin graphics.

Typeface conventions

This publication uses the following typeface conventions:

Bold

- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text
- Interface controls (check boxes, push buttons, radio buttons, spin buttons, fields, folders, icons, list boxes, items inside list boxes, multicolumn lists, containers, menu choices, menu names, tabs, property sheets) and labels (such as **Tip:** and **Operating system considerations**:)
- Keywords and parameters in text

Italic

- Citations (examples: titles of publications, diskettes, and CDs)
- Words defined in text (example: a nonswitched line is called a *point-to-point line*)
- Emphasis of words and letters (words as words example: "Use the word *that* to introduce a restrictive clause."; letters as letters example: "The LUN address must start with the letter *L*.")
- New terms in text (except in a definition list): a *view* is a frame in a workspace that contains data.
- Variables and values you must provide: ... where *myname* represents....

Monospace

- Examples and code examples
- File names, programming keywords, and other elements that are difficult to distinguish from surrounding text
- Message text and prompts addressed to the user
- Text that the user must type
- Values for arguments or command options

Operating system-dependent variables and paths

This publication uses the UNIX convention for specifying environment variables and for directory notation.

When using the Windows command line, replace **$***variable* with **%** *variable***%** for environment variables and replace each forward slash (**/**) with a backslash (\) in directory paths. The names of environment variables are not always the same in the Windows and UNIX environments. For example, %TEMP% in Windows environments is equivalent to $TMPDIR in UNIX environments.

Note: You can use the UNIX conventions if you are using the bash shell on a Windows system.

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.

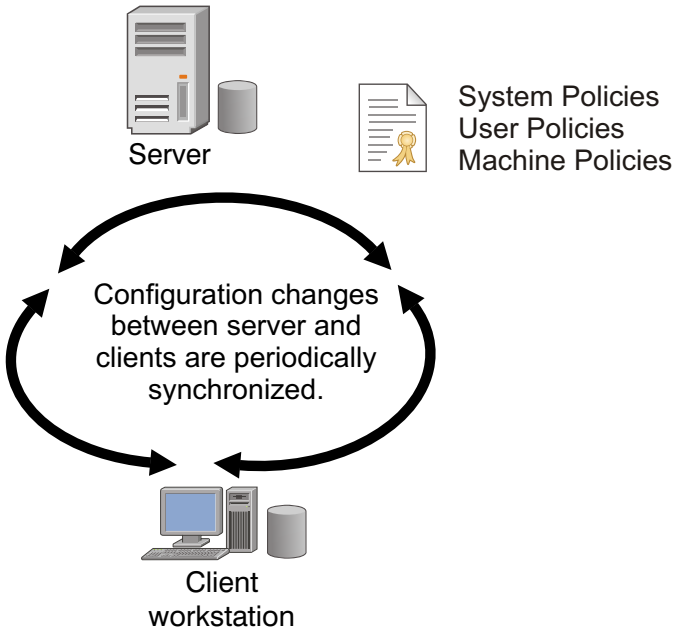

Figure 1. An overview of how different policies are synchronized between client and server in IBM Security Access Manager for Enterprise Single Sign-On.

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 later in this section.

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 125 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 specified by the policy. The product version that implements this policy is also indicated.
Location	Specifies the location of the policy. • For new policies: – **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: – **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: – **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): • `[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	The scope of applicability of the policy. **Values:** •  **System**: Policy is system-wide •  **Machine**: Policy affects only a specific machine •  **User**: Policy affects only a specific user
Note	The refresh frequency is indicated here. This value indicates when a policy will be effective after it is changed. • **Refreshed on use**: Policy read from the IMS Server or registry every time it is used. Changes, for example, are effective immediately. • **Refreshed on sync**: Policy read from the IMS Server or registry entry only on the next synchronization with the IMS Server. • **Refreshed on logon**: Policy read from the IMS Server or registry entry only on the next AccessAgent logon. • **Refreshed on startup**: Policy 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 upgrading 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 executing 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 such as smart cards, hybrid smart cards, RFIDs, ARFIDs, and fingerprints.

See "AccessAgent policies" on page 65 for more details about smart card, hybrid smart card, RFID, active proximity badge, 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 supported on this machine. This policy also controls the Wallet registration policy and imposes a constraint on the Wallet locks available for logon. **Note:** 1. If there is a GINA or Credential Provider installed, this policy is only updated on machine 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 machine restart to implement the changes.
Registry	
Type	String list MULTI_SZ
Values	• RFID • ARFID • Smart card • Hybrid smart card • Fingerprint
Scope	Machine
Note	• 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
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:** 1. This policy does not enforce the authentication factors 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. RFID includes active proximity badges or ARFID. 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	• Password • Password + RFID • Fingerprint • Smart card
Scope	User
Note	• 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 log on 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	• Yes • 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.

See the following topics for more information.

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 follows 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, such as periodic password change.
Registry	
Type	Boolean
Values	• Yes • 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	• Yes • 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:** Effective only if password expiry reminder is enabled.
Registry	
Type	Non-negative integers
Values	5 (default value)
Scope	System
Note	• 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 logging on to IBM Security Access Manager for Enterprise Single Sign-On. **Note:** Effective only if password periodic change is enabled.
Registry	
Type	Boolean
Values	• Yes • 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:** 1. For option 2, the links in the EnGINA welcome screen and AccessAgent UI is removed if no user is logged on. 2. The options only affect AccessAgent. AccessAssistant and Web Workplace are not affected by the policy.
Registry	
Type	Non-negative integer
Values	• Enable password reset link (default value) • 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:** 1. For option 2, the links in the EnGINA welcome screen, EnGINA locked screen, AccessAgent UI, and AccessAgent Tray right-click menu are removed. 2. If the password is configured to expire, the user is prompted to change password during logon. 3. If the Active Directory password synchronization is enabled and the Active Directory password expires, the user is prompted to change the password. 4. If changing password is forced during initial logon, the user sees the password change prompt upon initial logon. 5. The options only affect AccessAgent. AccessAssistant and Web Workplace are not affected by the policy.
Registry	
Type	
Values	• Enable password change link (default value) • 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:** 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, 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	• Yes (default value) • No
Scope	System
Note	Refreshed on logon.

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 AD password synchronization.

pid_enc_pwd_min_length

IMS Entry	Minimum password length
Location	**AccessAdmin** > **System** > **System policies** > **Password Policies** > **Password Strength Policies**
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	• Value ranges from 1 to 99. • Refreshed on sync.

pid_enc_pwd_max_length

Location	**AccessAdmin** > **System** > **System policies** > **Password Policies** > **Password Strength Policies**

pid_enc_pwd_max_length

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	
IMS Entry	Maximum password length
Type	Positive integer
Values	20 (default value)
Scope	System
Note	• 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	• Value ranges from 0 to 99. • Refreshed on sync.

pid_enc_pwd_min_alphabets_length

IMS Entry	Minimum number of alphabetic characters
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	• 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 uppercase and lowercase 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	• Yes • 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.

See the following topics for more information.

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	• Yes • No (default value)
Scope	System
Note	

pid_secrets_register_for_selfhelp_max

IMS Entry	Maximum number of secret questions a user should 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 for use in self-service workflows.
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 a user needs to answer to use self-service.
Location	**AccessAdmin** > **System** > **System policies** > **Self-service Policies** > **Self-service Password Reset Policies**
Description	The number of secret questions a user needs to 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 tries 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 authorization code generation policies

Know the different self-service authorization code policies, where to find and set these policies, their descriptions, and their default values. These policies apply only if the IMS Server is already configured to support the self-service authorization code generation feature.

pid_selfhelp_authcode_enabled

IMS Entry	Enable self-service authorization code generation?
Location	**AccessAdmin** > **System** > **System policies** > **Self-service Policies** > **Self-service Authorization Code Generation Policies**
Description	Whether to enable self-service authorization code issuance using a mobile phone.
Registry	
Type	Boolean
Values	• Yes • No (default value)
Scope	System
Note	Refreshed on use.

pid_selfhelp_authcode_request_from_any_phone_enabled

IMS Entry	Allow authorization code request from any phone?
Location	**AccessAdmin** > **System** > **System policies** > **Self-service Policies** > **Self-service Authorization Code Generation Policies**
Description	Whether to allow self-service authorization code to be requested from any phone. **Note:** Effective only if `pid_selfhelp_authcode_enabled` is **True**.
Registry	
Type	Boolean
Values	• Yes • No (default value)
Scope	System
Note	Refreshed on use.

pid_selfhelp_authcode_invalid_trial_count_max

IMS Entry	The maximum number of invalid attempts allowed before self-service authorization code request locks out
Location	**AccessAdmin** > **System** > **System policies** > **Self-service Policies** > **Self-service Authorization Code Generation Policies**
Description	The maximum number of allowed attempts using wrong authorization codes before the self-service authorization code request capability is locked. **Note:** Effective only if `pid_selfhelp_authcode_enabled` is **True**.
Registry	
Type	Positive integer
Values	6 (default value)
Scope	System
Note	Refreshed on use.

pid_selfhelp_authcode_request_help_text

IMS Entry	Help text for self-service authorization code request
Location	**AccessAdmin** > **System** > **System policies** > **Self-service Policies** > **Self-service Authorization Code Generation Policies**
Description	Configurable help text for self-service authorization code request. **Note:** 1. Effective only if `pid_selfhelp_authcode_enabled` is **True**. 2. The help text can be sent to the user through the SMS gateway IMS Bridge, shown by AccessAgent. 3. This message is available in multiple languages. It is displayed in the language specified by the user during AccessAgent installation.
Registry	
Type	String
Values	You can only request for an authorization code using a registered phone. The message format is: UserName UserSecret [RequestCode] (default value)

pid_selfhelp_authcode_request_help_text

Scope	System
Note	Refreshed on use.

pid_selfhelp_authcode_issue_msg_text

IMS Entry	Message text for self-help authorization code issuance
Location	**AccessAdmin** > **System** > **System policies** > **Self-service Policies** > **Self-service Authorization Code Generation Policies**
Description	Configurable message text for self-help authorization code issuance. **Note:** 1. Effective only if `pid_selfhelp_authcode_enabled` is **True**. 2. Use $AUTHCODE as placeholder for the authorization code. 3. Use $VALIDITY as placeholder for the number of valid days for the authorization code. 4. Use $USAGE as placeholder for a string that describes how the authorization code can be used. 5. This message is available in multiple languages. It is displayed in the language specified by the user during an AccessAgent installation.
Registry	
Type	String
Values	Your authorization code is $AUTHCODE. You can use it within $VALIDITY days for $USAGE. (default value)
Scope	System
Note	Refreshed on use.

pid_selfhelp_authcode_error_msg_text

IMS Entry	Error message text for self-help authorization code request
Location	**AccessAdmin** > **System** > **System policies** > **Self-service Policies** > **Self-service Authorization Code Generation Policies**
Description	Configurable error message text for self-help authorization code request. **Note:** 1. Effective only if `pid_selfhelp_authcode_enabled` is **True**. 2. This message is available in multiple languages. It is displayed in the language specified by the user during AccessAgent installation.
Registry	
Type	String
Values	An error has occurred. Contact your Helpdesk. (default value)
Scope	System
Note	Refreshed on use.

pid_selfhelp_authcode_different_phone_issue_msg_text

IMS Entry	Message text sent to requesting phone if it is different from registered phone

pid_selfhelp_authcode_different_phone_issue_msg_text

Location	**AccessAdmin** > **System** > **System policies** > **Self-service Policies** > **Self-service Authorization Code Generation Policies**
Description	Configurable message text that is sent to the requesting phone for self-help authorization code. The message is sent if the requesting phone is different from the registered phone. **Note:** 1. Effective only if `pid_selfhelp_authcode_enabled` is **True** and `pid_selfhelp_authcode_request_from_any_phone_enabled` is **False**. 2. Use $PHONE as a placeholder for a registered phone number. 3. This message is available in multiple languages. It is displayed in the language specified by the user during AccessAgent installation.
Registry	
Type	String
Values	An authorization code has been sent to your registered phone $PHONE. (default value)
Scope	System
Note	Refreshed on use.

pid_selfhelp_authcode_different_phone_error_msg_text

IMS Entry	Message text sent to requesting phone if it is different from registered phone and only registered phone can be used
Location	**AccessAdmin** > **System** > **System policies** > **Self-service Policies** > **Self-service Authorization Code Generation Policies**
Description	Configurable message text that is sent to the requesting phone for self-help authorization code. The message is sent if the requesting phone is different from the registered phone and the policy is that only the registered phone can be used. **Note:** 1. Effective only if `pid_selfhelp_authcode_enabled` is **True** and `pid_selfhelp_authcode_request_from_any_phone_enabled` is **False**. 2. Use $PHONE as a placeholder for a registered phone number. 3. This message is available in multiple languages. It is displayed in the language specified by the user during AccessAgent installation.
Registry	
Type	String
Values	An authorization code can only be requested from a registered phone $PHONE. (default value)
Scope	System
Note	Refreshed on use.

pid_selfhelp_authcode_wrong_credentials_error_msg_text

IMS Entry	Message text sent to requesting phone on incorrect credentials
Location	**AccessAdmin** > **System** > **System policies** > **Self-service Policies** > **Self-service Authorization Code Generation Policies**

pid_selfhelp_authcode_wrong_credentials_error_msg_text

Description	Configurable message text that is sent to the requesting phone for self-help authorization code if any of the requesting credentials are not correct. **Note:** 1. Effective only if `pid_selfhelp_authcode_enabled` is **True**. 2. Message text is sent if any of the requesting credentials is not correct(for example, user name, user secret, request code). 3. This message is available in multiple languages. It is displayed in the language specified by the user during an AccessAgent installation.
Registry	
Type	String
Values	Incorrect user name, user secret, or request code. Try again. (default value)
Scope	System
Note	Refreshed on use.

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 2nd 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:** 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
Values	• Yes • 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?

pid_second_factor_for_sign_up_required

Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **Sign Up Policies**
Description	Whether a second factor is required during sign up. **Note:** 1. Enable this policy if a second factor is required during sign up. Second authentication factors 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	`[DO] "SecondFactorForSignUpRequired"`
Type	DWORD
Values	• Yes • 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	Whether to enable automatic sign up. **Note:** 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 accordingly 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 logging on to an unregistered user name. The user is not prompted to confirm sign up if an unregistered second factor is presented.
Registry	`[DO] "AutomaticSignUpEnabled"`
Type	DWORD
Values	• Yes • 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**

pid_bind_secret_question_list

Description	The set of questions that the user chooses from during sign up to provide the secret answer. **Note:** 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 specified by the user during an AccessAgent installation.
Registry	
Type	String list
Values	• 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	• 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 additional secrets, because the primary secret is sufficient for performing self-service actions. The user can still choose to register more secrets after logging on by clicking **Set self-service secrets** in AccessAgent.
Registry	
Type	Boolean
Values	• Yes • No (default value)

pid_secrets_register_for_selfhelp_at_sign_up

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, must be specified by the user during sign up, or automatically specified using a bind task. **Note:** 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 vulnerabilities before deciding to implement 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. However, there is no support for migration from policy value `1` to `0`.
Registry	
Type	Non-negative integer
Values	• #0: Secret not required. • #1: Secret required, and user must specify during sign up.
Scope	System
Note	Refreshed on sync.

Chapter 7. Policies for Configurable Text and Accessibility

This section provides all the policies 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 specified by the user during an AccessAgent installation.

See the following topics for more information.

- "Configurable text policies"
- "Accessibility policy" on page 41

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.

See the following topics for more information.

- "EnGINA text policies"
- "Unlock text policies" on page 29
- "Sign up text policies" on page 40
- "AccessAssistant and Web Workplace text policies" on page 40

EnGINA 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 EnGINA welcome message. **Note:** 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 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	• 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** > **EnGINA Text Policies**
Description	Configurable text that is displayed right above the logon credentials when the user clicks **Log on**. **Note:** 1. If `pid_enc_pwd_is_ad_pwd_enabled` is set to **True**, this policy must be modified accordingly, 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 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	• 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** > **EnGINA Text Policies**
Description	Configurable text for password logon. **Note:** See `pid_engina_welcome_text`.
Registry	
Type	String list
Values	To log on, click 'Log on'.
Scope	System
Note	• 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** > **EnGINA 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	• 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
Location	**AccessAdmin** > **System** > **System policies** > **Configurable Text Policies** > **EnGINA 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	• 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
Location	**AccessAdmin** > **System** > **System policies** > **Configurable Text Policies** > **EnGINA 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	• 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_arfid_text

IMS Entry	Instructions for active proximity badge logon (Maximum 2 lines)
Location	**AccessAdmin** > **System** > **System policies** > **Configurable Text Policies** > **EnGINA Text Policies**
Description	Configurable text for active proximity badge logon. **Note:** See `pid_engina_welcome_text`.
Registry	
Type	String list
Values	To log on, present your active proximity badge. To log on without fingerprint, click 'Log on'.
Scope	System
Note	• 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** > **EnGINA 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	• 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 EnGINA bypass
Location	**AccessAdmin** > **System** > **System policies** > **Configurable Text Policies** > **EnGINA Text Policies**
Description	Configurable text message for automatic EnGINA bypass. **Note:** This message is available in multiple languages. It is displayed in the language 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 automatic sign-on will be 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** > **EnGINA 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	• 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**

pid_unlock_text

Description	Configurable text for a computer locked message. **Note:** 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 specified by the user during anAccessAgent installation.
Registry	
Type	String list
Values	This computer is protected by ISAM ESSO AccessAgent, and has been locked.
Scope	System
Note	• 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 to be displayed right above the unlock credentials when the user clicks **Unlock this computer**. **Note:** 1. If password is Active Directory password is set to **True**, this policy must be modified accordingly, 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 specified by the user during an AccessAgent installation.
Registry	
Type	String list
Values	Enter your user name and password to unlock.
Scope	System
Note	• 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)

pid_unlock_with_pwd_option_1_text

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	• 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**
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	• 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

pid_unlock_with_pwd_option_4_text

Values	To unlock, click 'Unlock this computer'.
Scope	System
Note	• 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'
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
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	• 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'
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

pid_unlock_with_sc_option_3_text

Note	• 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'
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
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	• 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'
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, insert your hybrid smart card. If you do not have your hybrid smart card, click 'Unlock this computer'.
Scope	System
Note	• 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 unlock policy is 'any user with or without current desktop account in Wallet can unlock'
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, insert your hybrid smart card. If you do not have your hybrid smart card, click 'Unlock this computer'.
Scope	System
Note	• 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'
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, insert your hybrid smart card. If you do not have your hybrid smart card, click 'Unlock this computer'.
Scope	System
Note	• 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**

pid_unlock_with_rfid_option_1_text

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	• 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	• 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

pid_unlock_with_rfid_option_4_text

Values	To unlock, tap your RFID card. If you do not have your RFID card, click 'Unlock this computer'.
Scope	System
Note	• Each text box can contain about 40 characters per line, and contain a maximum of 15 lines. • Refreshed on sync.

pid_unlock_with_arfid_option_1_text

IMS Entry	Instructions for unlocking with active proximity badge 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 active proximity badge when the computer is locked and `pid_unlock_option` is 1. **Note:** See `pid_unlock_text`.
Registry	
Type	String list
Values	To unlock, present your active proximity badge. To unlock without active proximity badge, click 'Unlock this computer'.
Scope	System
Note	• 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_arfid_option_3_text

IMS Entry	Instructions for unlocking with active proximity badge 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 active proximity badge when the computer locked and `pid_unlock_option` is 3. **Note:** See `pid_unlock_text`.
Registry	
Type	String list
Values	To unlock, present your active proximity badge. To unlock without active proximity badge, click 'Unlock this computer'.
Scope	System

pid_unlock_with_arfid_option_3_text

Note	• 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_arfid_option_4_text

IMS Entry	Instructions for unlocking with active proximity badge 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 active proximity badge when the computer is locked and `pid_unlock_option` is 4. **Note:** See `pid_unlock_text`.
Registry	
Type	String list
Values	To unlock, present your active proximity badge. To unlock without active proximity badge, click 'Unlock this computer'.
Scope	System
Note	• 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_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`.
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	• 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	• 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'.
Scope	System
Note	• 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**

pid_unlock_with_fingerprint_or_rfid_option_1_text

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	• 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	• 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	

pid_unlock_with_fingerprint_or_rfid_option_4_text

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	• 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 title
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:** 1. The **Domain** field is shown if the enterprise directory is the Active Directory. 2. Other than the domain, the template can only support either one or two fields. 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 Workpace Text Policies**

pid_accessanywhere_otp_reset_link_text

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_aa_accessibility_animation_effect_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	• No • 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.

See the following topic 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 not used in Windows Vista and Windows 7, because private desktop is not used on these platforms.

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 sto enable automatic locking of the computer after **`AutoAdminLogon`** or **`ForceAutoLogon`**.
Registry	`[DO] "WinStartupAction"`
Type	DWORD
Values	• No action (default value) • 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 Vista and later versions. **Note:** Effective only if the client operating system is Microsoft Windows Vista and later versions, and if Fast User Switching is enabled.
Registry	`[DO] "WinFastUserSwitchingEnabled"`
Type	Boolean

pid_win_fast_user_switching_enabled

Values	• Yes • No (default value)
Scope	Machine
Note	• Refreshed on sync. • For Windows Vista and Windows 7 systems 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	Maximum number of concurrent user sessions. Set it to 2 or a higher value to enable private desktop. **Note:** 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 DeploymentOptions.reg file during an AccessAgent installation. 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. The buttons and Windows hot keys might also remain not enabled after AccessAgent is uninstalled. 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 `pid_logoff_manual_action` to 1 (Log off Windows). Manually logging off AccessAgent is equivalent to logging off the desktop session of the user. 6. Set `pid_unlock_with_win_option` to 0 as unlocking with Windows is not supported for Local User Session Management. Enable auto-admin logon to Windows. Set `pid_microsoft_auto_logon_enabled` to 1, `pid_microsoft_auto_logon_acct` to a local machine log on account, and `pid_win_startup_action` to 1, to lock the computer immediately after logon. 7. Modifying this policy requires a machine restart to implement the changes.
Registry	`[DO] "LUSMSessionsMax"`
Type	DWORD
Values	1 (default value)

pid_lusm_sessions_max

Scope	Machine
Note	• 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	Option for replacing existing user sessions. Intended for the scenario where a new user attempts to log on while the number of concurrent user sessions has reached the maximum allowed number of sessions. **Note:** 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 has been unlocked the least number of times is replaced. 4. For policy value 4, the session that has been 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 machine restart to implement the changes.
Registry	`[DO] "LUSMSessionReplacementOption"`
Type	DWORD
Values	• Disallow new user to log on • Replace least recently used (LRU) session (default value) • Replace most recently used (MRU) session • Replace least frequently used (LFU) session • Replace least used (LU) session
Scope	Machine
Note	• 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	List of single instance applications (SIA), such as applications that cannot run multiple simultaneous instances in a computer. **Note:** 1. Effective only if `pid_lusm_sessions_max` is greater than 1. 2. When a user starts any application in this list, AccessAgent performs the action specified by • `pid_lusm_sia_launch_option` (if the policy value is not `0`), or • the launch option of the application. 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. 3. 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. 4. 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`. 5. Modifying this policy requires a machine restart to implement the changes.
Registry	`[DO] "LUSMSiaList"`
Type	MULTI_SZ
Values	Each application occupies three lines as follows: • 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: – 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	• 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 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 in a computer. **Note:** 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 machine restart to implement the changes.
Registry	`[DO] "LUSMSiaLaunchOption"`
Type	DWORD
Values	• Use launch option of the application • Disallow second instance to start • Log off existing instance (default value) • Close existing instance • Prompt user whether to log off existing instance • Prompt user whether to close existing instance • 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:** 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 machine restart to implement the changes.
Registry	`[DO] "LUSMGenericAccountsEnabled"`
Type	DWORD

pid_lusm_generic_accounts_enabled

Values	• Yes • 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 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 appears in the list of users 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 to perform desktop maintenance when necessary.
Registry	`[DO] "LUSMAutoLogonAcctDisplayEnabled"`
Type	Boolean DWORD
Values	• Yes (default value) • No
Scope	Machine
Note	Refreshed on startup.

Chapter 9. Policies for Terminal Server/Citrix

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

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

See the following topic for more information.

- "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	`[DO] "TSLightweightMode"`
Type	DWORD
Values	• 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 65 for more details about network policies.

See the following topics for more information.

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. **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	• 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	Whether to enable a **Delete user Wallets** option by right-clicking on the AccessAgent icon in WNA. **Note:** 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 deleting 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	• 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	Whether to override machine policies using registry values. **Note:** 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	• 0 - No (default value) • 1 - Yes
Scope	Machine
Note	Refreshed on use.

Memory Reduction policy

Know the policy about memory reduction, where to find and set this policy, description, and values.

pid_memory_reduction_freq_secs

Location	**Registry Editor** > **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **IBM** > **ISAM ESSO** > **DeploymentOptions**
Description	Interval, in seconds, for periodic calls to reduce the physical memory used by various AccessAgent components. **Note:** 1. A policy value of `0` means that this feature is not enabled. 2. Modifying this policy requires a machine restart to implement the changes.
Registry	`[DO] "MemoryReductionFreqSecs"`
Type	DWORD
Values	0 (default value)
Scope	Machine
Note	Refreshed on startup.

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	`[DO] "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	`[DO] "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.
Registry	`[DO] "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	`[DO] "LogLevel"`
Type	DWORD
Values	• No logging • Severe errors only (default value) • Basic info • More info, including SOAP logs • 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	`[DO] "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.

See the following topics for more information.

- "Wallet policies"
- "AccessAgent policies" on page 65

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	• **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.
Registry	
Type	Boolean
Values	• Yes (default value) • No
Scope	User System
Note	Refreshed on sync.

pid_wallet_personal_app_sso_enabled

IMS Entry	Enable automatic sign-on for personal authentication services?
Location	• **AccessAdmin** > **User Policy Templates** > **New template** > **Create new policy template** > **Wallet Policies** • **AccessAdmin** > **System** > **System policies** > **Wallet Policies**
Description	Whether to enable automatic sign-on for personal authentication services.
Registry	
Type	Boolean
Values	• Yes (default value) • No
Scope	User System

pid_wallet_personal_app_sso_enabled

Note	Refreshed on use for user policy. Refreshed on sync for system policy.

pid_accessagent_pwd_display_option

IMS Entry	Option for displaying of 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.
Registry	
Type	Non-negative integer
Values	• Disallow displaying passwords. (default value) • Allow displaying personal passwords. • 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 **Show password** option. **Note:** The user is asked to enter password before the user can export passwords.
Registry	
Type	Non-negative integer
Values	• Disallow exporting passwords. (default value) • Allow exporting personal passwords. • Allow exporting both enterprise and personal passwords.
Scope	User
Note	Refreshed on sync.

pid_sso_user_control_enabled

IMS Entry	Allow user to enable/disable automatic sign-on?

pid_sso_user_control_enabled

Location	**AccessAdmin** > **User Policy Templates** > **New template** > **Create new policy template** > **Wallet Policies**
Description	Whether to allow the user to enable or not enable automatic sign-on. **Note:** If this policy is not enabled, the **Enable automatic sign-on** and **Disable automatic sign-on** options do not display in the AccessAgent UI.
Registry	`[DO] "SsoUserControlEnabled"`
Type	DWORD Boolean
Values	• Yes (default value) • 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	• Password • Password entry option • Application settings • Delete credential • 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 allowed on the machine. **Note:** 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 logging 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 enbled. In this case, it overrides `pid_wallet_caching_option`.
Registry	`[DO] "WalletCacheMax"`
Type	DWORD
Values	999999999 (default value)
Scope	Machine
Note	• 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 perform synchronization with the IMS Server before logging on to the Wallet. **Note:** If this policy is set to 1, AccessAgent performs synchronization: • before logging on to Windows (for EnGINA log on) • before running the logon script (for desktop logon and logon from an unlock screen)
Registry	`[DO] "WalletSyncBeforeLogonEnabled"`
Type	DWORD
Values	• Yes (default value) • 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:** 1. If enabled, the user and machine cached Wallets are tied to the machine where they have been created. The cached Wallets 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	`[DO] "WalletCacheSecurityEnabled"`
Type	DWORD
Values	• Yes • 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:** 1. Offline reset capability is automatically enabled if Wallet is cached. 2. Wallet is always cached on a Citrix or Terminal Server. 3. Wallet is always cached if the ESSO Network Provider is used (the machine policy `pid_en_network_provider_enabled` is set to 1). 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	• Disallow caching • Ask user (default value) • Always cache
Scope	System
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	Maximum period of inactivity, in days, allowed for a cached Wallet. After the specified period, the cached Wallet is automatically revoked. **Note:** 1. The cached Wallet is automatically revoked on the IMS Server if it has exceeded the maximum number of days for inactivity. AccessAgent automatically revokes expired cached Wallets during each periodic synchronization, as long as 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 has not been 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 has been revoked. The option to cache the Wallet depends on `pid_wallet_caching_option`.
Registry	
Type	Positive integer
Values	999999999 (default value)
Scope	System
Note	• Set to 999999999 for infinity; cached Wallets do not expire. • Refreshed on sync.

pid_wallet_sync_mins

IMS Entry	Interval, in minutes, for synchronization of Wallet with IMS Server
Location	**AccessAdmin** > **System** > **System policies** > **Wallet Policies**
Description	Interval, in minutes, for periodic synchronization of the Wallet with the IMS Server. Synchronization is also performed 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 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 automatic sign-on password entry option
Location	**AccessAdmin** > **System** > **System policies** > **Wallet Policies**
Description	Default automatic sign-on password entry option.
Registry	
Type	Positive integer
Values	• Automatic log on • Always (default value) • Ask • Never • Certificate
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 is enabled.
Registry	
Type	Boolean
Values	• Yes (default value) • 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**

pid_migration_stage

Description	Whether migration from Tivoli Information Archive Manager version 1.x to 3.x is in progress and if applicable, the current stage of migration. **Note:** 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 have been upgraded. 4. The Wallets are upgraded as and when the user log 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.
Registry	
Type	Non-negative integer
Values	• No migration or migration completed. (default value) • Upgrading ISAM ESSO IMS Server and AccessAgent. • 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	Whether to perform a Wallet cleanup activity every time a new Wallet is cached. **Note:** 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: 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: • 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 perform cleanup.
Registry	`[DO] "WalletCleanupOnCachingEnabled"`
Type	DWORD
Values	• disabled • enabled
Scope	Machine
Note	

AccessAgent policies

View the details of the different policies that you can set forAccessAgent.

You can configure the following policies for AccessAgent:

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 AccessAgent bubble pop-ups at the Windows notification area.
Registry	`[DO] "AATrayBubbleDisplayEnabled"`
Type	Boolean DWORD
Values	• Yes (default value) • No
Scope	Machine
Note	Refreshed on use.

pid_aa_tray_menu_options_enabled

IMS Entry	Enable right-click menu options?

pid_aa_tray_menu_options_enabled

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 on the AccessAgent icon at the Windows notification area.
Registry	
Type	
Values	• Yes (default value) • 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:** 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 machine restart to implement the changes.
Registry	`[DO] "SessionInfoDisplayFreqSecs"`
Type	DWORD
Values	0 (default value)
Scope	Machine
Note	• 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**

pid_aa_feedback_link

Description	Enables the **Feedback** link in the AccessAgent user interface, which launches an e-mail client or Web browser. **Note:** • If the policy value is blank, (default) AccessAgent does not show the **Feedback** link. • If the policy value format is `mailto:abc@xyz.com`, clicking **Feedback** launches the default e-mail client of the user and the e-mail is sent to `abc@xyz.com`. • If the policy value format is `http://xyz.com`, clicking **Feedback** launches the default browser of the user and navigates to `http://xyz.com`.
Registry	`"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** > **Temp**
Description	Default IMS Server name.
Registry	`[DIMS] "ImsServerName"`
Type	SZ
Values	
Scope	Machine
Note	Refreshed on use.

EnGINA policies

Know the different policies for EnGINA, 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** > **EnGINA Policies**
Description	Whether to enable the option to go to Windows logon directly from EnGINA.
Registry	`[DO] "EnginaWinlogonOptionEnabled"`
Type	DWORD
Values	• Yes (default value) • No
Scope	Machine
Note	Refreshed on use.

pid_engina_app_launch_enabled

IMS Entry	Enable application launch from EnGINA?
Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **EnGINA Policies**
Description	Whether to enable the launching of an application from the EnGINA welcome or locked screen.
Registry	`[DO] "EnginaAppLaunchEnabled"`
Type	DWORD
Values	• Yes • 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** > **EnGINA Policies**
Description	Display label for the link on EnGINA welcome or locked screen, for launching an application. **Note:** Effective only if `pid_engina_app_launch_enabled` is 1.
Registry	`[DO] "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** > **EnGINA Policies**
Description	Command line for launching an application from an EnGINA welcome or locked screen. **Note:** 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**.
Registry	`[DO] "EnginaAppLaunchCmd"`
Type	SZ
Values	
Scope	Machine
Note	Refreshed on use.

pid_engina_bypass_hot_key_enabled

IMS Entry	Enable EnGINA Bypass Hot Key?
Location	• **AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **EnGINA Policies** • **AccessAdmin** > **System** > **System policies** > **AccessAgent Policies** > **EnGINA Policies**
Description	Whether the EnGINA Bypass Hot Key is enabled. **Note:** 1. If enabled, the user can press the EnGINA Bypass Hot Key sequence to bypass EnGINA and go to Windows to log on or unlock. 2. The Hot Key is accepted at any of the following EnGINA 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_lusm_sessions_max` is greater than 1). 5. Modifying this policy requires a machine restart to implement the changes.
Registry	`[DO] "EnginaBypassHotKeyEnabled"`
Type	DWORD Boolean
Values	• Yes (default value) • No
Scope	Machine System
Note	Refreshed on startup.

pid_engina_bypass_hot_key_sequence

IMS Entry	EnGINA Bypass Hot Key sequence
Location	• **AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **EnGINA Policies** • **AccessAdmin** > **System** > **System policies** > **AccessAgent Policies** > **EnGINA Policies**
Description	The EnGINA Bypass Hot Key sequence. **Note:** 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	`[DO] "EnginaBypassHotKeySequence"`
Type	MULTI_SZ String list

pid_engina_bypass_hot_key_sequence

Values	• Ctrl • Alt • Home
Scope	Machine System
Note	You can select a maximum of three keys from this set except Ctrl+Alt+Del: • Ctrl • Shift • Alt • Ins • Del • Home • End • PgUp • PgDn • Break • E 2 of the keys in this set must be used so that the probability of conflict with other applications is minimized: Ctrl, Shift, Alt Refreshed on startup.

pid_engina_bypass_automatic_enabled

IMS Entry	Enable automatic EnGINA bypass?
Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **EnGINA Policies**
Description	Whether automatic EnGINA Bypass is enabled. **Note:** 1. If this policy is enabled, the IMS Server is not accessible, and the user Wallet is not cached, AccessAgent automatically bypasses EnGINA. 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: • `pid_enc_pwd_is_ad_pwd_enabled` is `True` • IMS Server is not accessible • Wallet of the user is not cached 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. 3. This feature does not support logon with second factors. 4. Modifying this policy requires a machine restart to implement the changes.
Registry	`[DO] "EnginaBypassAutomaticEnabled"`

pid_engina_bypass_automatic_enabled

Type	DWORD
Values	• Yes • No (default value)
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	• **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 might perform a set of actions.
Registry	`[DO] "DesktopInactivityMins"`
Type	DWORD Positive integer
Values	30 (default value)
Scope	Machine System
Note	• Refreshed on sync for system policy. • Refreshed on use for machine policy.

pid_desktop_inactivity_action

IMS Entry	Desktop inactivity actions
Location	• **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_desktop_inactivity_action

Description	Actions to be performed by AccessAgent after a period of desktop inactivity. **Note:** 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	`[DO] "DesktopInactivityAction"`
Type	DWORD Non-negative integer
Values	• No action (default value) • Log off Windows • Log off Wallet • Lock computer • Log off Wallet and lock computer
Scope	Machine System
Note	• 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	• **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.
Registry	`[DO] "DesktopInactivityActionCountdownSecs"`
Type	DWORD Non-negative integer
Values	5 (default value)
Scope	Machine System
Note	• 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	• **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	Actions to be performed by AccessAgent on Windows screen saver activation. **Note:** 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: • 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 then the computer does the following actions: • shows the screen saver after 2 minutes of no user activity • locks the computer after an additional 2 minutes of no user activity **Important:** • The screensaver action is not supported in Microsoft Windows Vista. • Option `0` is not supported in Microsoft Windows Vista.
Registry	`[DO] "WinScreensaverAction"`
Type	DWORD Non-negative integer
Values	• Disable Windows screen saver • If screen saver is password protected, lock computer, else show normal screen saver • Lock computer (default value)
Scope	Machine System
Note	• Refreshed on sync for system policy. • Refreshed on use for machine policy. AccessAgent assumes that `ScreenSaverGracePeriod` is 0 when it locks the workstation and screen saver activation. If the user dismisses the screensaver before the grace period is over, the machine remains unlocked, but the lock scripts are executed.

pid_locked_computer_inactivity_mins

IMS Entry	Locked computer inactivity duration, in minutes

pid_locked_computer_inactivity_mins

Location	• **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 might perform a set of actions.
Registry	`[DO] "LockedComputerInactivityMins"`
Type	DWORD Positive integer
Values	30 (default value)
Scope	Machine System
Note	• Refreshed on sync for system policy. • Refreshed on use for machine policy.

pid_locked_computer_inactivity_action

IMS Entry	Locked computer inactivity actions when user is logged on to Wallet
Location	• **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	AccessAgent performs the specified actions after a period of desktop inactivity when the computer is locked and the user is logged on to a Wallet. **Note:** 1. Effective only if `pid_lusm_sessions_max` is 1. 2. This policy is effective only if the EnGINA screen lock is shown.
Registry	`[DO] "LockedComputerInactivityAction"`
Type	DWORD Non-negative integer
Values	• No action (default value) • Log off Windows
Scope	Machine System
Note	• Refreshed on sync for system policy. • Refreshed on use for machine policy.

Lock/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**
Description	Whether to enable the running of the lock script when locking the AccessAgent session of the user. **Note:** 1. The lock script is only executed if the session of the user is currently 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 executed 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: • be running before locking. • be relaunched during unlock. **Important:** When using Microsoft Windows Vista: • The lock script is executed after the machine locks instead of before the machine locks. • The user is not prompted for action upon machine lock.
Registry	
Type	Boolean
Values	• Yes • 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	Type of lock script to run. **Note:** 1. Effective only if `pid_script_lock_enabled` is enabled. 2. See `pid_script_lock_enabled`.
Registry	
Type	Positive integer
Values	• Batch (default) • VBScript

pid_script_lock_type

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 only executed if the user has an existing AccessAgent session and is unlocking the session. 2. The unlock script is not executed if the user is unlocking a shared workstation that is: • 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 executed instead. 3. The unlock script can be used in Local User Session Management. The script can automatically launch single-instance applications that might have been 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	• Yes • No (default value)
Scope	User

pid_script_unlock_enabled

Note	Refreshed on sync.

pid_script_unlock_type

IMS Entry	Unlock script 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	• Batch (default) • 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	• **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	Unlock computer policy for controlling who can unlock a computer when it has been locked by a user who is logged on to AccessAgent. **Note:** 1. Effective only if `pid_lusm_sessions_max` is `1`. 2. Same user refers to the same user who locked the computer. 3. This policy is ignored if `pid_lock_option` is `2` (transparent screen lock). In transparent screen lock mode, any user can unlock the computer. 4. 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. 5. 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 currently not supported for ARFID and smart card. **Important:** Limitations for Microsoft Windows Vista users: • Option `3` only works with a Shared Desktop. • Option `4` logs off the current AccessAgent logon session without attempting to log on again as a second user.
Registry	`[DO] "UnlockOption"`
Type	DWORD Positive integer
Values	• Only the same user can unlock • Any user with or without current desktop account Wallet can unlock (default value) • Only the same user can unlock, but different user can re-log on to Windows
Scope	Machine User
Note	• 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	• **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. **Note:** 1. Effective only if `pid_lusm_sessions_max` is 2. 2. Effective when a user attempts to unlock a computer when another user has already been 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	`[DO] "UnlockDifferentUserActionCountdownSecs"`
Type	DWORD Non-negative integer
Values	0 - to not enable confirmation countdown
Scope	Machine User
Note	• 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:** 1. If `pid_lusm_sessions_max` is greater than 1, only policy 1 (EnGINA 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 actions specified by `pid_logoff_manual_action` is performed. 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 specified by `pid_desktop_inactivity_action` is still carried out after the period of desktop inactivity has elapsed. Then, set `pid_desktop_inactivity_action` to 4. **Important:** The transparent screen lock feature is not supported in Microsoft Windows Vista.
Registry	`[DO] "LockOption"`
Type	DWORD
Values	• EnGINA screen lock (default) • Transparent screen lock
Scope	Machine

pid_lock_option

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	`[DO] "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:** 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	`[DO] "LockTransparentHotKeyEnabled"`
Type	DWORD
Values	• Yes • 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 using Windows unlock. **Note:** 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 using Windows unlock.
Registry	[DO] "UnlockWithWinOption"
Type	DWORD
Values	• 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 Tivoli Access Manager for Enterprise Single Sign-On Windows unlock prompt with a user name. • 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 will be pre-filled with the currently logged on user name. If no user is logged on to AccessAgent, the unlock prompt will be 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	[DO] "UnlockUserNamePrefillOption"
Type	DWORD
Values	• Use the user name pre-fill option for logon prompt (default value) • Prefill with currently logged on or last logged on user name Registry values: • 0 - Use the user name pre-fill option for logon prompt • 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 check?
Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **AccessAgent Policies** > **Lock/Unlock Policies**

pid_fast_unlock_enabled

Description	Whether to allow AccessAgent to unlock a computer without performing any checks with the IMS Server.
Registry	
Type	Boolean
Values	• 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	• **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 performed when a smart card is removed.
Registry	
Type	Non-negative integer
Values	• Log off Windows • Log off Wallet • Lock computer (default value) • 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	Whether to allow smart card users to log on to Windows using certificate-based authentication. **Note:** 1. If enabled, after the user logs on to AccessAgent from the Welcome screen, the user can log on to Windows using 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 Vista.
Registry	

pid_sc_win_logon_enabled

Type	Boolean
Values	• Yes • No (default value)
Scope	Machine
Note	Refreshed on sync.

pid_sc_map_cert_to_entdir_acc_enabled

IMS Entry	Enable automatic mapping of certificate to 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 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	• Yes • No (default value)
Scope	System
Note	Refreshed on sync.

pid_engina_ui_enabled

IMS Entry	Enable 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	• Yes (default value) • 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?

pid_sc_1f_unlock_enabled

Location	**AccessAdmin** > **Machine Policy Templates** > **New Template** > **AccessAgent Policies** > **Smart card PoliciesAccessAdmin** > **User Policy Template** > **New Template** > **AccessAgent Policies** > **Smart card Policies**
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	• True: Enabled • False: Not enabled (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 PoliciesAccessAdmin** > **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	• >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 has recently logged on using smart card and PIN on the same computer or another computer. This policy applies if logon happens in the duration specified by the single factor smart card logon timeout.
Registry	
Type	Boolean
Values	• True: Enabled • False: Not enabled (default value)

pid_sc_1f_logon_enable

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, single factor smart card logon is not allowed.
Registry	
Type	Non-negative integer
Values	• >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 a user logs on with a smart card and PIN before grace period expires.
Registry	
Type	
Values	• No • Yes
Scope	Machine User
Note	

pid_sc_present_same_action

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

pid_sc_present_same_action

Type	Non-negative integer
Values	• 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, for presenting the same smart card on the desktop
Location	**AccessAdmin** > **Machine Policy Templates** > **New Template** > **AccessAgent Policies** > **Smart card PoliciesAccessAdmin** > **User Policy Template** > **New Template** > **AccessAgent Policies** > **Smart card Policies**
Description	Confirmation countdown duration, in seconds, for presenting the same smart card on the desktop.
Registry	
Type	Non-negative integer
Values	• 0: No countdown • >0: Countdown in seconds **Note:** 5 is the default value.
Scope	Machine User
Note	

pid_sc_present_different_action

IMS Entry	Actions on presenting different smart card on desktop if user logged on with single factor
Location	**AccessAdmin** > **Machine Policy Templates** > **New Template** > **AccessAgent Policies** > **Smart card PoliciesAccessAdmin** > **User Policy Template** > **New Template** > **AccessAgent Policies** > **Smart card Policies**
Description	Actions on presenting a different smart card on the desktop. 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_different_action

Values	• 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
Scope	Machine User
Note	

pid_sc_present_different_action_countdown_secs

IMS Entry	Confirmation countdown duration, in seconds, for presenting a different smart card on the desktop
Location	**AccessAdmin** > **Machine Policy Templates** > **New Template** > **AccessAgent Policies** > **Smart card PoliciesAccessAdmin** > **User Policy Template** > **New Template** > **AccessAgent Policies** > **Smart card Policies**
Description	Confirmation countdown duration, in seconds, for presenting a different smart card on the desktop.
Registry	
Type	Non-negative integer
Values	• 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 tapping same RFID on desktop
Location	• **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_tap_same_action

Description	Actions to be performed by AccessAgent when the currently logged on user taps the RFID card on the desktop. **Note:** 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	`[DO] "RfidTapSameAction"`
Type	DWORD Non-negative integer
Values	• No action (default value) • Log off Windows • Log off Wallet • Lock computer • Log off Wallet and lock computer
Scope	Machine User
Note	• 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, for tapping same RFID on desktop
Location	• **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, for tapping the same RFID on the desktop.
Registry	`[DO] "RfidTapSameActionCountdownSecs"`
Type	DWORD Non-negative integer
Values	5 (default value)
Scope	Machine User
Note	• 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	• **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	Whether to allow RFID-only unlock (without password) by the same user who locked the computer, if unlock happens in a specified duration. This policy also applies to Active Proximity Badge.
Registry	`[DO] "RfidOnlyUnlockEnabled"`
Type	DWORD Boolean
Values	• Yes • No (default value)
Scope	Machine User
Note	• 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	• **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	Time expiry, in seconds, for an RFID-only unlock. After this duration (timed from the last lock), RFID-only unlock is not allowed. **Note:** 1. Effective only if `pid_rfid_only_unlock_enabled` is enabled. 2. Also applies to Active Proximity Badge.
Registry	`[DO] "RfidOnlyUnlockTimeoutSecs"`
Type	DWORD Non-negative integer
Values	0 (default value)
Scope	Machine User
Note	• 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**
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:** 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	• Set value to `0` if RFID-only logon is not enabled. • Refreshed on sync.

pid_rfid_tap_different_action

IMS Entry	Actions on tapping different RFID on desktop
Location	• **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 performed by AccessAgent when an RFID card is tapped on the desktop and does not belong to the currently logged on user. **Note:** 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 logging off 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. **Important:** Limitation for Microsoft Windows Vista and Windows 7 users: 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.

pid_rfid_tap_different_action

Registry	`[DO] "RfidTapDifferentAction"`
Type	DWORD Non-negative integer
Values	• No action (default value) • Lock computer • Log off Wallet and lock computer • Switch user • Log off Windows and log on as new user
Scope	Machine User
Note	• 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, for tapping different RFID on desktop
Location	• **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, for tapping a different RFID on the desktop.
Registry	`[DO] "RfidTapDifferentActionCountdownSecs"`
Type	DWORD Non-negative integer
Values	5 (default value)
Scope	Machine User
Note	• 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	Whether to allow RFID-only logon (without password):
	• by a user who has recently logged on using an RFID and password on the same or another computer
	• if logon happens in the duration specified by `pid_rfid_only_logon_timeout_mins`
	Note:
	1. RFID-only logon only works 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:
	  • 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 time-out has expired.
	  • If no user is logged on and the computer is locked: When a user taps 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	`[DO] "RfidOnlyLogonEnabled"`
Type	DWORD
Values	• Yes • 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	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. **Note:** 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 only works when a user is logged on to AccessAgent.
Registry	`[DO] "RfidDisplayUtilityEnabled"`
Type	DWORD

pid_rfid_display_utility_enabled

Values	• Yes • No (default value)
Scope	Machine
Note	Refreshed on use.

Active Proximity Badge policies

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

pid_arfid_presentation_range_max

IMS Entry	Maximum range for recognizing that an active proximity badge is presented
Location	• **AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **Active Proximity Badge Policies** • **AccessAdmin** > **System** > **System policies** > **AccessAgent Policies** > **Active Proximity Badge Policies**
Description	Maximum range for detecting an active proximity badge.
Registry	`[DO] "ArfidPresentationRangeMax"`
Type	Positive integer
Values	3 (default value)
Scope	Machine System
Note	• The value can range from 1 to 16. • The minimum range for an Active Proximity Badge removal is 3. • A value of 3 is set for the closest proximity, 5 is for medium proximity, and 7 for the farthest proximity. • Refreshed on use.

pid_arfid_removal_range_min

IMS Entry	Minimum range for recognizing that an active proximity badge is removed
Location	• **AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **Active Proximity Badge Policies** • **AccessAdmin** > **System** > **System policies** > **AccessAgent Policies** > **Active Proximity Badge Policies**
Description	Minimum range for detecting the removal of an active proximity badge.
Registry	`[DO] "ArfidRemovalRangeMin"`
Type	Positive integer
Values	7 (default value)
Scope	Machine System

pid_arfid_removal_range_min

Note	• The value can range from 4 to 19. • The maximum range of Active Proximity Badge presentation 3. • A value of 7 is set for the closest proximity, 9 for medium proximity, and 13 for the farthest proximity. • 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 tapping same finger on desktop
Location	• **AccessAdmin** > **User Policy Templates** > **AccessAgent Policies** > **Fingerprint Policies** • **AccessAdmin** > **Machine Policy Templates** > **AccessAgent Policies** > **Fingerprint Policies**
Description	Actions to be performed by AccessAgent when the currently logged on user places a finger on the reader. **Note:** 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	`[DO] "FingerprintTapSameAction"`
Type	DWORD Non-negative integer
Values	• No action (default value) • Log off Windows • Log off Wallet • Lock computer • Log off Wallet and lock computer
Scope	Machine User
Note	• 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, for tapping same finger on desktop

pid_fingerprint_tap_same_action_countdown_secs

Location	• **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, for placing the same finger on the fingerprint reader.
Registry	`[DO] "FingerprintTapSameActionCountdownSecs"`
Type	DWORD Non-negative integer
Values	5 (default value)
Scope	Machine User
Note	• 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 tapping different finger on desktop
Location	• **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	Actions to be performed by AccessAgent when a finger is tapped on the desktop and does not belong to the currently logged on user. **Note:** 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 logging 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. **Important:** Limitation for Microsoft Windows Vista users: For option `8`, AccessAgent logs off the current logon session without attempting to log on again as a second user.
Registry	`[DO] "FingerprintTap DifferentAction"`

pid_fingerprint_tap_different_action

Type	DWORD Non-negative integer
Values	• No action (default value) • Lock computer • Log off Wallet and lock computer • Switch user • Log off Windows and log on as new user
Scope	Machine User
Note	• 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, for tapping different finger on desktop
Location	• **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, for placing a different finger on the fingerprint reader.
Registry	`[DO] "FingerprintTapDifferentActionCountdownSecs"`
Type	DWORD Non-negative integer
Values	5 (default value) 0 (not enable confirmation countdown)
Scope	Machine User
Note	• 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
Location	**AccessAdmin** > **System** > **System policies** > **AccessAgent Policies** > **Fingerprint Policies**

pid_fingerprint_registration_max

Description	Maximum number of fingerprints that each user is allowed to register. **Note:** A user who has 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, if attempting 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	• 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 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 perform validation after logon, enable background authentication.
Registry	
Type	Positive integer
Values	• Yes (default value) • No
Scope	Machine
Note	• 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 has been 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 using 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?
Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **Terminal Server Policies**

pid_ts_logon_prompt_enabled

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	`[DO] "TSLogonPromptEnabled"`
Type	DWORD
Values	• Yes • No (default value)
Scope	Machine
Note	Refreshed on use.

pid_ts_engina_logon_no_local_session_enabled

IMS Entry	Use EnGINA 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 EnGINA logon or Microsoft GINA logon for the Terminal Server session, when there is no local AccessAgent session. **Note:** 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	`[DO] "TSEnginaLogonNoLocalSessionEnabled"`
Type	DWORD
Values	• Yes • No (default value)
Scope	Machine
Note	Refreshed on use.

pid_ts_aa_menu_option

IMS Entry	Option for displaying menu options on 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	`[DO] "TSAaMenuOption"`
Type	DWORD
Values	• 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 must perform 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 machine restart to implement the changes.
Registry	`[DO] "ComRedirEnabled"`
Type	DWORD
Values	• Yes • No (default value)
Scope	Machine
Note	Refreshed on startup.

pid_com_redir_local_virtual_port

IMS Entry	Virtual COM port on 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	`[DO] "ComRedirLocalVirtualPort"`
Type	DWORD
Values	1 (default value)
Scope	Machine
Note	• The value can range from 1 to 8. • Refreshed on startup.

pid_com_redir_remote_physical_port

IMS Entry	Physical COM port on 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:** 1. Effective only if `pid_com_redir_enabled` is 1. 2. Modifying this policy requires a machine restart to implement the changes.
Registry	`[DO] "ComRedirRemotePhysicalPort"`
Type	DWORD
Values	1 (default value)
Scope	Machine
Note	• 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:** 1. This policy must be set on the remote AccessAgent (such as on the Terminal Server or Citrix server). 2. This policy only applies to launching of published applications. 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 machines that do not have a local AccessAgent installed (for example, home or Internet café).
Registry	`[DO] "TSStartAANoLocalAAEnabled"`
Type	DWORD
Values	• Yes (default value) • 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:** 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: • 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 logon to remote AccessAgent is performed using credentials 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): • policy value `0` on a Terminal Server or Citrix server installation. • policy value `1` on a client machine installation. Modifying this policy requires a machine restart to implement the changes.
Registry	`[DO] "MachineTypeTS"`
Type	DWORD
Values	• Machine is Terminal Server • Machine is not Terminal Server (default value)
Scope	Machine
Note	Refreshed on startup.

pid_ts_delay_app_launch_exe_list

IMS Entry	
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 perform automatic sign-on. **Note:** 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	`[DO] "TSDelayAppLaunchExeList"`
Type	MULTI_SZ
Values	
Scope	Machine
Note	Refreshed on use.

pid_ts_delay_app_launch_enabled

IMS Entry	
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:** 1. This feature is only applicable to Citrix. It is not applicable to Terminal Server access using 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 perform automatic 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 perform automatic 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	`[DO] "TSDelayAppLaunchEnabled"`
Type	DWORD
Values	• Yes • No (default value)
Scope	Machine

pid_ts_delay_app_launch_enabled

Note	Refreshed on use.

pid_ts_delay_app_launch_timeout_secs

IMS Entry	
Location	**Registry Editor** > **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **IBM** > **ISAM ESSO** > **DeploymentOptions**
Description	Timeout, in seconds, for delaying an application launch. **Note:** 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 automatic sign-on to be ready. If a remote AccessAgent is not ready for automatic 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	`[DO] "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 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

pid_ts_lock_local_computer_action

Values	• No action (default value) • Disconnect remote session • Log off remote AccessAgent and disconnect remote session • Log off remote session • 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 logging off from the local AccessAgent.
Registry	
Type	Non-negative integer
Values	• No action • Disconnect remote session • Log off remote AccessAgent and disconnect remote session (default value) • Log off remote session • 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	• Yes • 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
Values	• 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	• Yes • No (default value)
Scope	User
Note	Refreshed on sync.

pid_script_logoff_type

IMS Entry	Logoff script type

pid_script_logoff_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
Values	• Batch (default) • 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	• **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 a user to manually log off from AccessAgent. **Note:** If this policy is not enabled, the **Log off AccessAgent** option does not display in theAccessAgent UI.
Registry	`[DO] "LogoffManualEnabled"`
Type	DWORD Boolean
Values	• Yes (default value) • No
Scope	Machine User
Note	Refreshed on sync.

pid_logoff_manual_action

IMS Entry	Actions on manual logoff by user
Location	• **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 performed by AccessAgent on a manual logoff by the user. **Note:** 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 fromAccessAgent. 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	`[DO] "LogoffManualAction"`
Type	DWORD Positive integer
Values	• Log off Windows • Log off Wallet (default value) • Log off Wallet and lock computer
Scope	Machine User
Note	• 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	• **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. **Note:** 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.

pid_logoff_manual_action_countdown_secs

Registry	`[DO] "LogoffManualActionCountdownSecs"`
Type	DWORD Non-negative integer
Values	30 (default value)
Scope	Machine User
Note	• 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	Whether to enable the Network Provider (`EnNetworkProvider`). **Note:** 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	`[DO] "EnNetworkProviderEnabled"`
Type	DWORD
Values	• Yes • 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**

pid_logon_user_name_prefill_option

Description	Option for pre-filling the IBM Security Access Manager for Enterprise Single Sign-On logon prompt with a user name. **Note:** 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"`
Registry	`[DO] "LogonUserNamePrefillOption"`
Type	DWORD
Values	• Do not prefill. • Prefill with last logged on user name. (default value) • 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	Option for displaying the name of the currently logged on user. **Note:** 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 only display about 20 characters. 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 so on), 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	`[DO] "LogonUserNameDisplayOption"`
Type	DWORD
Values	• User name (default value) • Given name followed by family name • 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**
Description	Timeout, in seconds, for logging off from applications. **Note:** 1. 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. 2. 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	`[DO] "LogoffAppTimeoutSecs"`
Type	DWORD
Values	5 (default value)
Scope	Machine
Note	• 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 for all applications when a user logs off from AccessAgent. **Note:** 1. 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 logoff is not performed. 2. 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. 3. This policy is effective when a user is logged off from AccessAgent, for example, during a switch user operation.
Registry	
Type	Positive integer
Values	• Log off the application • Close the application • 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	• **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	Whether the IBM Security Access Manager for Enterprise Single Sign-On Hot Key is enabled. **Note:** 1. From EnGINA, 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	`[DO] "EncHotKeyEnabled"`
Type	DWORD Boolean
Values	• Yes (default value) • No
Scope	Machine System
Note	Refreshed on startup.

pid_enc_hot_key_sequence

IMS Entry	ISAM ESSO Hot Key sequence
Location	• **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	The IBM Security Access Manager for Enterprise Single Sign-On Hot Key sequence. **Note:** 1. Effective only if `pid_enc_hot_key_enabled` is enabled. 2. Modifying this policy requires a machine restart to implement the changes.
Registry	`[DO] "EncHotKeySequence"`
Type	MULTI_SZ String list

pid_enc_hot_key_sequence

Values	• Ctrl • Alt • E
Scope	Machine System
Note	• 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	• **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	Actions to be performed by AccessAgent if the IBM Security Access Manager for Enterprise Single Sign-On Hot Key is pressed from a desktop when a user is logged on to AccessAgent. **Note:** 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	`[DO] "EncHotKeyAction"`
Type	DWORD Non-negative integer
Values	• No action • Log off Windows • Log off Wallet • Lock computer • Log off Wallet and lock computer • Launch AccessAgent window (default value)
Scope	Machine System
Note	• 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 ISAM ESSO Hot Key
Location	• **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. **Note:** 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	`[DO] "EncHotKeyActionCountdownSecs"`
Type	DWORD Non-negative integer
Values	5 (default value)
Scope	Machine System
Note	• 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	• **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	Actions to be performed 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. **Note:** 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.

pid_enc_hot_key_not_logged_on_action

Registry	`[DO] "EncHotKeyNotLoggedOnAction"`
Type	DWORD Non-negative integer
Values	• No action • Log off Windows • Lock computer • Launch AccessAgent window (default value)
Scope	Machine System
Note	• 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.

pid_emergency_hot_key_enabled

IMS Entry	Enable Emergency Hot Key?
Location	• **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	Whether the Emergency Hot Key is enabled. **Note:** 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.
Registry	`[DO] "EmergencyHotKeyEnabled"`
Type	DWORD Boolean
Values	• Yes • No (default value)
Scope	Machine System
Note	Refreshed on startup.

pid_emergency_hot_key_sequence

IMS Entry	Emergency Hot Key sequence
Location	• **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. **Note:** 1. Effective only if Emergency Hot Key is enabled. 2. Modifying this policy requires a machine restart to implement the changes. **Important:** Emergency bypass unlock is not supported in Microsoft Windows Vista.
Registry	`[DO] "EmergencyHotKeySequence"`
Type	MULTI_SZ String list
Values	• Ctrl • Alt • End
Scope	Machine System
Note	• 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.

Presence detector policies

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

pid_presence_detector_enabled

IMS Entry	Enable presence detector?
Location	• **AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **Presence Detector Policies** • **AccessAdmin** > **System** > **System policies** > **AccessAgent Policies** > **Presence Detector Policies**
Description	Whether to enable a presence detector. **Note:** 1. This policy does not automatically turn on or turn off the third-party presence detector hardware and software. 2. Modifying this policy requires a machine restart to implement the changes.

pid_presence_detector_enabled

Registry	`[DO] "PresenceDetectorEnabled"`
Type	DWORD Boolean
Values	• Yes • No (default value)
Scope	Machine System
Note	Refreshed on startup.

pid_presence_detector_walk_away_key_sequence

IMS Entry	Key sequence sent by presence detector when user walks away
Location	• **AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **Presence Detector Policies** • **AccessAdmin** > **System** > **System policies** > **AccessAgent Policies** > **Presence Detector Policies**
Description	The key sequence that the presence detector sends when a user walks away from the computer. **Note:** 1. Effective only if `pid_presence_detector_enabled` is enabled. 2. The same key sequence must be configured on the presence detector by using vendor software. For RF IDeas pcProx-Sonar, configure the **Walkaway Keystrokes** using the pcProx-Sonar Configuration Utility. 3. Modifying this policy requires a machine restart to implement the changes.
Registry	`[DO] "PresenceDetectorWalkAwayKeySequence"`
Type	MULTI_SZ String list
Values	• Ctrl • Alt • PgDn
Scope	Machine System
Note	• 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.

pid_presence_detector_walk_away_action

IMS Entry	Actions performed by AccessAgent when presence detector detects user walking away while logged on
Location	• **AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **Presence Detector Policies** • **AccessAdmin** > **System** > **System policies** > **AccessAgent Policies** > **Presence Detector Policies**
Description	Actions to be performed by AccessAgent when a presence detector detects a user walking away while no user is logged on. **Note:** 1. Effective only if `pid_presence_detector_enabled` is enabled. 2. 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 desktop session and shows the computer locked screen.
Registry	`[DO] "PresenceDetectorWalkAwayAction"`
Type	DWORD Non-negative integer
Values	• No action • Log off Windows • Log off Wallet • Lock computer (default value) • Log off Wallet and lock computer
Scope	Machine System
Note	• Refreshed on sync for system policy. • Refreshed on use for machine policy.

pid_presence_detector_walk_away_action_countdown_secs

IMS Entry	Confirmation countdown duration, in seconds, when presence detector detects user walking away
Location	• **AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **Presence Detector Policies** • **AccessAdmin** > **System** > **System policies** > **AccessAgent Policies** > **Presence Detector Policies**
Description	Confirmation countdown duration, in seconds, when the presence detector detects a user walking away from the computer. **Note:** Effective only if `pid_presence_detector_enabled` is enabled.
Registry	`[DO] "PresenceDetectorWalkAwayActionCountdownSecs"`
Type	DWORD Non-negative integer
Values	5 (default value)

pid_presence_detector_walk_away_action_countdown_secs

Scope	Machine System
Note	• If you do not want to enable confirmation countdown, set this value to `0`. • Refreshed on sync for system policy. • Refreshed on use for machine policy.

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	`[DO] "AuditLogByAAEnabled"`
Type	DWORD
Values	• Yes (default value) • No
Scope	Machine
Note	Refreshed on sync.

Background authentication policies

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

pid_background_auth_enabled_option

IMS Entry	Option to perform background authentication
Location	**AccessAdmin** > **Machine Policies** > **AccessAgent Policies** > **Logon/Logoff Policies**
Description	Option to specify if AccessAgent must perform authentication with the IMS Server in the background.
Registry	
Type	Non-negative integer
Values	• 0 - Never • 1 - Only when the user logs on offline or performs fast unlock
Scope	Machine

pid_background_auth_enabled_option

Note	**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. • 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	• 0 - Do not reattempt 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 perform AccessAgent tasks from Web browsers by using Web Workplace. AccessAssistant contains automatic sign-on functionalities without installing AccessAgent on a computer.

See the following topic 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	• Yes (default value) • 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 when using AccessAssistant.
Registry	
Type	Boolean
Values	• Yes (default value) • 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	• Yes • No (default value)
Scope	User
Note	Refreshed on sync.

pid_accessanywhere_app_sso_enabled

IMS Entry	Enable automatic sign-on to applications in AccessAssistant?
Location	**AccessAdmin** > **System** > **System policies** > **AccessAssistant and Web Workplace Policies**
Description	Whether the user can perform automatic sign-on to applications through AccessAssistant.
Registry	
Type	Boolean
Values	• Yes • 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	• Yes • No (default value)

pid_accessanywhere_edit_user_profile_enabled

Scope	System
Note	Refreshed on sync.

pid_accessanywhere_sync_mins

IMS Entry	Interval, in minutes, for periodic synchronization of AccessAssistant and Web Workplace with 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 displaying application passwords in AccessAssistant.
Registry	
Type	Non-negative integer
Values	• Disable viewing of passwords • Display password, no option to copy to clipboard • Display password by default, with option to copy to clipboard (default) • 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:** 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 entering the user name and password. The MAC is sent through the preferred channel of the user. A message indicates where the MAC has been 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	• Authorization code • MAC • 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	• Yes • 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.

See the following topics for more information.

- "Application policies"
- "Authentication service policies" on page 127

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 performing automatic sign-on?
Location	**AccessAdmin** > **System** > **Application policies** > **<*Application name*>** > **Application Policies**
Description	Whether another password authentication is required before performing automatic sign-on for the application. **Note:** Override authentication or authenticate again with a password.

pid_app_reauth_with_enc_pwd_enabled

Registry	
Type	Boolean
Values	• Yes • No (default value)
Scope	System
Note	Refreshed on sync.

pid_app_inject_pwd_entry_option_default

IMS Entry	Default automatic sign-on password entry option for the application
Location	**AccessAdmin** > **System** > **Application policies** > **<*Application name*>** > **Application Policies**
Description	Default automatic sign-on password entry option for the application. **Note:** Overrides authentication inject password entry option default and Wallet inject password entry option default.
Registry	
Type	Positive integer
Values	• Automatic log on • Always (default value) • Ask • Never • Certificate • Use application settings
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. **Note:** 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. Internet Explorer (IE) is also considered an application. In this context, the web application policy overrides the IE policy, which overrides Wallet logoff action for applications default. 4. Set the policy to 2 and 3 for Internet Explorer and Windows Explorer. 5. This policy is set to 3 for Windows logon (application GINA) when the IMS Server is installed.
Registry	
Type	Positive integer

pid_app_wallet_logoff_action

Values	• Log off the application • Close the application • Do nothing (default value)
Scope	System
Note	Refreshed on use.

Authentication service policies

View the details of the different authentication service policies.

These are the different policies you can configure for authentication service:

- "Password policies"
- "Authentication policies" on page 131

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 a manual password change with a random password is enabled for the authentication service.
Registry	
Type	Boolean
Values	• Yes • No (default value)
Scope	User
Note	Refreshed on sync.

pid_auth_reauth_with_enc_pwd_enabled

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

pid_auth_reauth_with_enc_pwd_enabled

Values	• Yes • 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	• Yes • 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	• 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)
Scope	System

pid_enc_pwd_max_length

Note	• 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	• 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	• 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	Minimum 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
Values	0 (default value)
Scope	System

pid_auth_fortification_pwd_min_special_characters_length

Note	• 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	• 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	• 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	• 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	• Yes • 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	• Yes • No (default value)
Scope	System
Note	Refreshed on sync.

pid_auth_inject_pwd_entry_option_default

IMS Entry	Default automatic sign-on password entry option for the authentication service

pid_auth_inject_pwd_entry_option_default

Location	**AccessAdmin** > **System** > **Authentication service policies** > **<*Authentication service name*>** > **Authentication Policies**
Description	Default automatic 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	• Automatic log on • Always (default value) • Ask • Never • 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	• Password (default value) • SCR • CAPI • OTP (ISAM ESSO) • MAC • CCOW • OTP (time-based) • OTP (OATH)
Scope	System
Note	• You can select multiple values. • Refreshed on sync.

pid_auth_capture_prompt_enabled

IMS Entry	Prompt user on auto-capture of password?

pid_auth_capture_prompt_enabled

Location	**AccessAdmin** > **System** > **Authentication service policies** > **<*Authentication service name*>** > **Authentication Policies**
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	• Yes (default value) • No
Scope	System
Note	Refreshed on sync.

pid_auth_accounts_max

IMS Entry	Maximum number of accounts allowed for the authentication service
Location	• **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 has reached or exceeded the maximum specified by this policy: 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 has 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	• 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.

See the following topic 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	• 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	ActiveCode authentication bypass option. **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	• Authorization code and password • Authorization code and enterprise account password • 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	• MAC only (no appending of secret) (default value) • MAC + password • MAC + Enterprise account password • MAC + Administrator- assigned secret • Password + MAC • Enterprise account password + MAC • 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:** 1. Not applicable to AA-OTP. 2. The order is also specified in the policy values.
Registry	
Type	Non-negative integer
Values	• OTP only (no appending of secret) (default value) • OTP + password • OTP + Enterprise account password • OTP + Administrator- assigned secret • Password + OTP • Enterprise account password + OTP • 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:** 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	• The value can range from 1 to 5. • Refreshed on use.

Chapter 15. 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	`[DO] "AAOnlineHelpLink"`
Type	REG_SZ
Values	IBM Security Access Manager for Enterprise Single Sign-On Infocenter (default value)
Scope	
Note	Set this policy to empty to remove the Help link from the AccessAgent user interface.

Location	**Registry Editor** > **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **IBM** > **ISAM ESSO** > **ECSS** > **DeploymentOptions**
Description	Controls the Help link on the Observer window.
Registry	`[DO] "ObsOnlineHelpEnabled"`
Type	DWORD
Values	• 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	`[DO] "WindowsEventLogEnabled"`
Type	DWORD
Values	• 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	`[DO] "SystemModalMessageEnabled"`
Type	DWORD
Values	• 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	`[DO] "UIDirectionLToR"`
Type	DWORD
Values	• 0 - False • 1 - True (default value)
Scope	
Note	

Appendix. 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 `pid_fast_user_switching_enabled` 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 `pid_fast_user_switching_enabled` 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 (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.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 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.

Index

U

V

W

Printed in USA

SC23-9694-01