IBM® Security Access Manager for Enterprise Single Sign-On
Version 8.2.2

Policies Definition Guide

IBM® Security Access Manager for Enterprise Single Sign-On
Version 8.2.2

Policies Definition Guide

Note
Before using this information and the product it supports, read the information in "Notices" on page 125.

Edition notice

Note: This edition applies to version 8.2.2 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.

© Copyright IBM Corporation 2002, 2015.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

About this publication v
Accessibility v
Technical training. v
Support information. v
Statement of Good Security Practices v

Chapter 1. Policies in AccessAdmin. . . 1

Chapter 2. Policy legends 3

Chapter 3. Viewing and setting policy priorities 5
Viewing policy priorities 5
Setting policy priorities. 5

Chapter 4. Policies for Authentication Factors 7
Authentication policies 7

Chapter 5. Policies for Password Management. 9
Password aging policies 9
Password change policies. 11
Password strength policies 12

Chapter 6. Policies for Sign up and Password Reset. 15
Self-service password reset policies 15
Self-service registration and bypass of second factor policies. 16
Sign up policies 17

Chapter 7. Policies for Configurable Text and Accessibility 21
Configurable text policies. 21
ESSO Credential Provider text policies 21
Unlock text policies. 25
Sign up text policies 35
Accessibility policy 36

Chapter 8. Policies for Private and Shared desktops 37
Shared workstation policies 37

Chapter 9. Policies for Citrix and Terminal Server 39
Lightweight mode policy 39

Chapter 10. Policies for Debugging Management and Control. 41
Auditing policies 41
Troubleshooting policies 41
Temporary file policy 43
Log policies 43

Chapter 11. Policies for Wallet and AccessAgent 45
Wallet policies 45
AccessAgent policies 53
Display policies 53
ESSO Credential Provider policies 55
Desktop inactivity policies 59
Lock and Unlock policies. 63
Smart card policies 71
Hybrid smart card policies 72
RFID policies. 76
Fingerprint policies. 83
Terminal Server policies 87
Roaming session policies 93
Log on/Log off policies 94
Hot Key policies 100
Audit logging policies 104
Background authentication policies 104
Network policies 105

Chapter 12. Policies for Applications and Authentication Services 107
Application policies 107
Authentication service policies 109
Password policies 109
Authentication policies 113

Chapter 13. Policies for Privileged Identity Management 117
IBM Security Privileged Identity Manager configuration policies. 117

Chapter 14. Other policies 121

Chapter 15. Policy limitations in Windows 7 and above 123

Notices 125

Glossary 129
A 129
B 130
C 130
D 131
E 132
F 132
G 132
H 132
I. 133

© Copyright IBM Corp. 2002, 2015

J. 133
K 133
L 133
M 133
N 134
O 134
P 134
R 135
S 135
T 137
U 137
V 137
W 138

Index 139

About this publication

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

Accessibility

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

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

Technical training

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

Support information

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

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

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

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

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and

© Copyright IBM Corp. 2002, 2015

may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Chapter 1. Policies in AccessAdmin

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

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

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

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

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

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

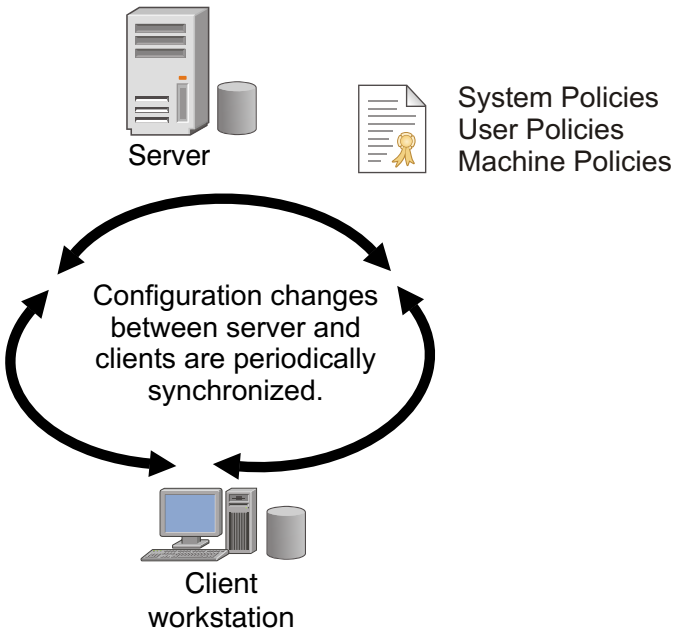

Figure 1. An overview of how different policies are synchronized between client and server in IBM Security Access Manager for Enterprise Single Sign-On.

Scope

The applicability of a policy is determined by scope.

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

© Copyright IBM Corp. 2002, 2015

Take note of the following information.

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

There are three ways to edit user policies in AccessAdmin.

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

Dependencies

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

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

In general, application-specific policies override authentication service-specific policies, which in turn, override general Wallet policies. The Wallet inject password entry option default policy (`pid_wallet_inject_pwd_entry_option_default`) is used when the other two policies are not defined for a particular authentication service or application. See Chapter 12, “Policies for Applications and Authentication Services,” on page 107 for more details.

Chapter 2. Policy legends

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

Attribute	Description
✔	Frequently used policies
Policy ID	Unique identifier of the policy.
IMS Entry	The entry in the IMS Server for System and User policies. If this column is blank, the value must be set in the registry. If not, the value indicates the name of the policy, which can be set in the IMS Server.
Description	Description of the policy, including a list of the possible behaviors that are specified by the policy. The product version that implements this policy is also indicated.
Location	Specifies the location of the policy. • 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.

© Copyright IBM Corp. 2002, 2015

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 that is read from the IMS Server or registry every time it is used. Changes, for example, are effective immediately. • **Refreshed on sync**: Policy that is read from the IMS Server or registry entry only on the next synchronization with the IMS Server. • **Refreshed on logon**: Policy that is read from the IMS Server or registry entry only on the next AccessAgent logon. • **Refreshed on startup**: Policy that is read from the IMS Server or registry entry only on system startup.

Chapter 3. Viewing and setting policy priorities

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

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

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

Viewing policy priorities

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

Before you begin

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

Procedure

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

Setting policy priorities

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

Procedure

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

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

© Copyright IBM Corp. 2002, 2015

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

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

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

Chapter 4. Policies for Authentication Factors

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

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: Authentication second factors supported

IMS Entry	Authentication second factors supported
Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **Authentication Policies**
Description	The second factors that are supported on this computer. This policy also controls the Wallet registration policy and imposes a constraint on the Wallet locks available for logon. **Note:** 1. If there is a Credential Provider installed, this policy is only updated on computer restart. 2. If there is no Credential Provider installed, this policy is only updated when a new Windows session is created. For example, when the user logs on to Windows and not when the user unlocks a Windows session. 3. Modifying this policy requires a computer restart to implement the changes. 4. This policy is only supported if **pid_auth_provider** is empty.
Type	String list MULTI_SZ
Values	• RFID • 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: Wallet authentication policy

IMS Entry	Wallet authentication policy
Location	**AccessAdmin** > **User Policy Templates** > **New template** > **Create new policy template** > **Authentication Policies**

© Copyright IBM Corp. 2002, 2015

pid_wallet_authentication_option: Wallet authentication policy

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 that are used for sign-up. The sign-up policy is enforced by `pid_second_factors_supported_list` and `pid_second_factor_for_sign_up_required`. 2. Smart card includes hybrid smart cards. 3. This policy is only supported if **pid_auth_provider** is empty.
Type	Positive integer list
Values	• #1: Password • #2: Password + RFID • #5: Fingerprint • #6: Smart card
Scope	User
Note	• You can select multiple values. • All values are supported for 32-bit AccessAgent. • Refreshed on logon or unlock by different user, if online. • Refreshed on sync.

pid_auth_provider: Authentication provider policy

IMS Entry	Authentication provider policy
Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new policy template** > **Authentication Policies**
Description	This policy specifies the authentication provider that is used to login to AccessAgent. **Note:** This policy is currently used to support Kerberos authentication.
Values	• Empty • SPNEGO: Enables Kerberos authentication in AccessAgent.
Scope	Machine
Note	Refreshed on startup.

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.

Password aging policies

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

pid_enc_pwd_periodic_change_enabled: Enable password aging?

IMS Entry	Enable password aging?
Location	**AccessAdmin** > **System** > **System policies** > **Password Policies** > **Password Aging Policies**
Description	Whether to enable password aging? User must do periodic password change.
Registry	
Type	Boolean
Values	• #True: Yes • #False: No (default value)
Scope	System
Note	Refreshed on sync.

pid_enc_pwd_change_days: Maximum password age, in 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**

© Copyright IBM Corp. 2002, 2015

pid_enc_pwd_expiry_reminder_enabled

Description	Whether to remind the user about the expiring password. **Note:** Effective only if password periodic change is enabled.
Registry	
Type	Boolean
Values	• #True: Yes • #False: No (default value)
Scope	System
Note	Refreshed on sync.

pid_enc_pwd_expiry_reminder_days: Number of days before password expiry to start reminding user

IMS Entry	Number of days before password expiry to start reminding user
Location	**AccessAdmin** > **System** > **System policies** > **Password Policies** > **Password Aging Policies**
Description	Number of days before password expiry to start reminding the user. **Note:** This policy is effective only if password expiry reminder is enabled.
Registry	
Type	Non-negative integers
Values	5 (default value)
Scope	System
Note	• Value ranges from 1 to 10. • Refreshed on sync.

pid_enc_pwd_expiry_change_enforced: Enforce password change on expiry?

IMS Entry	Enforce password change on expiry?
Location	**AccessAdmin** > **System** > **System policies** > **Password Policies** > **Password Aging Policies**
Description	Whether to enforce password change on expiry. The user is prompted to change the password before logon to IBM Security Access Manager for Enterprise Single Sign-On. **Note:** Effective only if password periodic change is enabled.
Registry	
Type	Boolean
Values	• #True: Yes • #False: No (default value)
Scope	System
Note	Refreshed on sync.

Password change policies

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

pid_enc_pwd_reset_option: Enable password reset?

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 ESSO Credential Provider welcome screen and AccessAgent UI is removed if no user is logged on. 2. The options affect AccessAgent only. AccessAssistant and Web Workplace are not affected by the policy.
Registry	
Type	Non-negative integer
Values	• #1: Enable password reset link (default value) • #2: Disable password reset link
Scope	System
Note	Refreshed on sync.

pid_enc_pwd_change_option: Enable changing of password?

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 ESSO Credential Provider welcome screen, ESSO Credential Provider 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 change password is forced during initial logon, the user sees the password change prompt upon initial logon. 5. The options affect AccessAgent only. AccessAssistant and Web Workplace are not affected by the policy.
Registry	
Type	
Values	• #1: Enable password change link (default value) • #2: Disable password change link
Scope	System
Note	Refreshed on sync.

pid_enc_pwd_change_on_first_logon_enabled: Force provisioned users to change the password at first logon?

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, the provisioned users are forced to change passwords according to the Active Directory setting for **User must change password at next logon**. 3. This feature is not supported for fingerprint logon.
Registry	
Type	Boolean
Values	• #True: Yes (default value) • #False: No
Scope	System
Note	Refreshed on logon.

pid_inject_winlogon_password_on_change_disabled: InjectWinlogonPasswordOnChangeDisabled

IMS Entry	
Location	**Registry Editor** > **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **IBM** > **ISAM ESSO** > **DeploymentOptions**
Description	Whether to disable the injection of the Windows login password to the Windows Change Password screen. **Note:** This policy is only applicable to Windows 7 and later.
Registry	`[DO] "InjectWinlogonPasswordOnChangeDisabled"`
Type	DWORD
Values	• #0: No (default value) • #1: Yes
Scope	Machine
Note	Refreshed on use.

Password strength policies

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

pid_enc_pwd_min_length: Minimum password length

IMS Entry	Minimum password length

pid_enc_pwd_min_length: 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: Maximum password length

IMS Entry	Maximum password length
Location	**AccessAdmin** > **System** > **System policies** > **Password Policies** > **Password Strength Policies**
Description	Maximum length of an acceptable password. **Note:** Not effective if Active Directory password synchronization is enabled. Active Directory password strength policies are used instead.
Registry	
Type	Positive integer
Values	20 (default value)
Scope	System
Note	• Value ranges from 1 to 99. • Refreshed on sync.

pid_enc_pwd_min_numerics_length: Minimum number of numeric characters

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: Minimum number of alphabetic characters

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: Enforce the use of both upper case and lower case characters?

IMS Entry	Enforce the use of both upper case and lower case characters?
Location	**AccessAdmin** > **System** > **System policies** > **Password Policies** > **Password Strength Policies**
Description	Whether to enforce the use of both upper case and lower case characters for the password. **Note:** Not effective if Active Directory password synchronization is enabled. Active Directory password strength policies are used instead.
Registry	
Type	Boolean
Values	• #True: Yes • #False: No (default value)
Scope	System
Note	Refreshed on sync.

Chapter 6. Policies for Sign up and Password Reset

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

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: Enable self-service password reset?

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	• #True: Yes • #False: No (default value)
Scope	System
Note	

pid_secrets_register_for_selfhelp_max: Maximum number of secret questions a user can register to enable self-service

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

pid_secrets_verify_for_selfhelp: The number of secret questions the user must answer to use self-service

IMS Entry	The number of secret questions the user must answer to use self-service.
Location	**AccessAdmin** > **System** > **System policies** > **Self-service Policies** > **Self-service Password Reset Policies**

© Copyright IBM Corp. 2002, 2015

pid_secrets_verify_for_selfhelp: The number of secret questions the user must answer to use self-service

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

pid_secrets_verify_invalid_trial_count_max: The maximum number of invalid login attempts allowed before self-service locks out

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

Self-service registration and bypass of second factor policies

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

pid_selfhelp_second_factor_registration_and_bypass_enabled: Enable self-service registration and bypass of second factor?

IMS Entry	Enable self-service registration and bypass of second factor?
Location	**AccessAdmin** > **System** > **System policies** > **Self-service Policies** > **Self-service Registration and Bypass of Second Factor Policies**
Description	Whether to enable self-service registration and bypass of a second factor. **Note:** 1. If this policy is enabled, the user can bypass the use of a second factor for logon by providing registered secrets. 2. If an authorization code is required for the second-factor registration, the user can do a self-service registration by providing registered secrets. 3. If the user cannot provide registered secrets, there is an option to provide an authorization code and the primary secret.
Registry	
Type	Boolean

pid_selfhelp_second_factor_registration_and_bypass_enabled: Enable self-service registration and bypass of second factor?

Values	• #True: Yes • #False: No (default value)
Scope	System
Note	Refreshed on sync.

Sign up policies

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

pid_second_factor_for_sign_up_required: Require authentication second factor during sign up?

IMS Entry	Require authentication second factor during sign up?
Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **Sign Up Policies**
Description	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 that are defined in the user policy template can be implemented only after user registration. 2. Effective only if the second factors supported list is not empty. In this case, any one of the supported second factors can be used for sign up. There is one UI dialog that requests the user to present any one of the supported second factors. 3. If policy value is 1, sign up fails if the second factor is not presented.
Registry	`[DO] "SecondFactorForSignUpRequired"`
Type	DWORD
Values	• #True: Yes • #False: No (default value)
Scope	Machine
Note	Refreshed on use.

pid_automatic_sign_up_enabled: Enable automatic sign up?

IMS Entry	Enable automatic sign up?
Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **Sign Up Policies**

pid_automatic_sign_up_enabled: Enable automatic sign up?

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 if this policy is set to 1. 3. If this policy is set to 1, the **Sign up** option is not available on both the AccessAgent UI and AccessAgent Tray menu. The user is not prompted to sign up if the user logs on to an unregistered user name. The user is not prompted to confirm sign up if an unregistered second factor is presented.
Registry	`[DO] "AutomaticSignUpEnabled"`
Type	DWORD
Values	• #True: Yes • #False: No (default value)
Scope	Machine
Note	Refreshed on use.

pid_bind_secret_question_list: Question set for secret

IMS Entry	Question set for secret
Location	**AccessAdmin** > **System** > **System policies** > **Sign Up Policies**
Description	The set of questions user can choose 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 that is 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: Minimum length of an acceptable secret answer

IMS Entry	Minimum length of an acceptable secret answer

pid_secret_answer_min_length: 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: Prompt user to register additional secrets for self-service during sign up?

IMS Entry	Prompt user to register additional secrets for self-service during sign up?
Location	**AccessAdmin** > **System** > **System policies** > **Sign Up Policies**
Description	Whether to prompt the user to register additional secrets for self-service during sign up. **Note:** If `pid_secrets_verify_for_selfhelp` is `1`, the user is not prompted to register more secrets, because the primary secret is sufficient for the self-service actions. The user can still choose to register more secrets after logon by clicking **Set self-service secrets** in AccessAgent.
Registry	
Type	Boolean
Values	• #True: Yes • #False: No (default value)
Scope	System
Note	Refreshed on sync.

pid_secret_option: Option for specifying secret

IMS Entry	Option for specifying secret
Location	**AccessAdmin** > **System** > **System policies** > **Sign Up Policies**
Description	Whether the secret is required, it must be specified by the user during sign up. **Note:** 1. This policy applies to users who are signing up or who are logging on for the first time after their accounts have been pre-provisioned. 2. For policy value `0`, the user is assigned a system-defined secret. The user is not prompted for a secret when performing actions that require it (for example, reset password and offline recovery). The customer must understand the security implications to using a system-defined secret before the implementation of such a configuration. 3. If the policy value is changed from `1` to `0`, the user is automatically migrated to a system-defined secret when the user logs on to AccessAgent successfully. 4. Once the policy value is set to `0` during sign-up, adding a user-defined primary secret later is not supported. You can only add user-defined primary secret during sign-up.

pid_secret_option: Option for specifying secret

Registry	
Type	Non-negative integer
Values	• #0: Secret not required. • #1: Secret required, and user must specify during sign up. (default)
Scope	System
Note	• When the **pid_auth_provider** policy is set, this policy must be set to 0. • Refreshed on sync.

Chapter 7. Policies for Configurable Text and Accessibility

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

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.

ESSO Credential Provider text policies

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

pid_engina_welcome_text: Welcome message

IMS Entry	Welcome message (Maximum 2 lines)
Location	**AccessAdmin** > **System** > **System policies** > **Configurable Text Policies** > **ESSO Credential Provider text policies**
Description	Configurable text for the ESSO Credential Provider 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 that is specified by the user during an AccessAgent installation.
Registry	
Type	String list
Values	This computer is protected by ISAM ESSO AccessAgent. If you are here for the first time, click 'Sign up' to get started.
Scope	System
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: Logon credentials message

IMS Entry	Logon credentials message (Maximum 1 line)
Location	**AccessAdmin** > **System** > **System policies** > **Configurable Text Policies** > **ESSO Credential Provider Text Policies**

© Copyright IBM Corp. 2002, 2015

pid_logon_credentials_text: Logon credentials message

Description	Configurable text that is to be 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, for example, `Enter your Windows domain user name and password to log on`. 2. This message is available in multiple languages. It is displayed in the language that is specified by the user during an AccessAgent installation.
Registry	
Type	String list
Values	Enter your user name and password to log on.
Scope	System
Note	• Maximum of 1 string. • Text box takes 2 lines max, about 40 characters per line. • Refreshed on sync.

pid_engina_logon_with_pwd_text: Instructions for password logon

IMS Entry	Instructions for password logon (Maximum 2 lines)
Location	**AccessAdmin** > **System** > **System policies** > **Configurable Text Policies** > **ESSO Credential Provider 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: Instructions for RFID logon

IMS Entry	Instructions for RFID logon (Maximum 2 lines)
Location	**AccessAdmin** > **System** > **System policies** > **Configurable Text Policies** > **ESSO Credential Provider 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'.

pid_engina_logon_with_rfid_text: Instructions for RFID logon

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: Instructions for smart card logon

IMS Entry	Instructions for smart card logon (Maximum 2 lines)
Location	**AccessAdmin** > **System** > **System policies** > **Configurable Text Policies** > **ESSO Credential Provider 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: Instructions for hybrid smart card logon

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

IMS Entry	Instructions for fingerprint logon (Maximum 2 lines)
Location	**AccessAdmin** > **System** > **System policies** > **Configurable Text Policies** > **ESSO Credential Provider 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: Message for automatic ESSO Credential Providerbypass

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

pid_engina_logon_with_fingerprint_or_rfid_text: Instructions for fingerprint or RFID logon

IMS Entry	Instructions for fingerprint or RFID logon (Maximum 2 lines)
Location	**AccessAdmin** > **System** > **System policies** > **Configurable Text Policies** > **ESSO Credential Provider 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'.

pid_engina_logon_with_fingerprint_or_rfid_text: Instructions for fingerprint or RFID logon

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: Locked computer message

IMS Entry	Locked computer message (Maximum 1 line)
Location	**AccessAdmin** > **System** > **System policies** > **Configurable Text Policies** > **Unlock Text Policies**
Description	Configurable text for a computer locked message. **Note:** 1. This message is displayed, followed by a blank line, and then messages in one of the configurable unlock text policies (depending on current Wallet and `pid_unlock_option`). 2. The two lines of messages are separated by a blank line. 3. "\n\n" can be added if more blank lines are necessary. 4. This message is available in multiple languages. It is displayed in the language that is specified by the user during an AccessAgent installation.
Registry	
Type	String list
Values	This computer is protected by ISAM ESSO AccessAgent, and has been locked.
Scope	System
Note	• 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: Unlock credentials message

IMS Entry	Unlock credentials message (Maximum 1 line)
Location	**AccessAdmin** > **System** > **System policies** > **Configurable Text Policies** > **Unlock Text Policies**

pid_unlock_credentials_text: Unlock credentials message

Description	Configurable text that is to be displayed right above the unlock credentials when the user clicks **Unlock this computer**. **Note:** 1. If Active Directory password synchronization is enabled, this policy must be modified. For example, `Enter your Windows domain user name and password to unlock`. 2. This message is available in multiple languages. It is displayed in the language that is specified by the user during an AccessAgent installation.
Registry	
Type	String list
Values	Enter your user name and password to unlock.
Scope	System
Note	• 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: Instructions for unlocking with password when unlock policy is 'only the same user can unlock'

IMS Entry	Instructions for unlocking with password when unlock policy is 'only the same user can unlock' (Maximum 2 lines)
Location	**AccessAdmin** > **System** > **System policies** > **Configurable Text Policies** > **Unlock Text Policies**
Description	Configurable text for unlocking with a password when the computer is locked and `pid_unlock_option` is 1. **Note:** See `pid_unlock_text`.
Registry	
Type	String list
Values	To unlock, click 'Unlock this computer'.
Scope	System
Note	• 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: Instructions for unlocking with password when unlock policy is 'any user with or without current desktop account in Wallet can unlock'

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

pid_unlock_with_pwd_option_3_text: Instructions for unlocking with password when unlock policy is 'any user with or without current desktop account in Wallet can unlock'

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: Instructions for unlocking with password when unlock policy is 'only the same user can unlock, but different user can re-log on to Windows'

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

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

pid_unlock_with_sc_option_1_text: Instructions for unlocking with smart card when unlock policy is 'only the same user can unlock'

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: Instructions for unlocking with smart card when unlock policy is 'any user with or without current desktop account in Wallet can unlock'

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

IMS Entry	Instructions for unlocking with smart card when unlock policy is 'only the same user can unlock, but different user can re-log on to Windows' (Maximum 2 lines)
Location	**AccessAdmin** > **System** > **System policies** > **Configurable Text Policies** > **Unlock Text Policies**

pid_unlock_with_sc_option_4_text: 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'

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: Instructions for unlocking with hybrid smart card when unlock policy is 'only the same user can unlock'

IMS Entry	Instructions for unlocking with hybrid smart card when unlock policy is 'only the same user can unlock' (Maximum 2 lines)
Location	**AccessAdmin** > **System** > **System policies** > **Configurable Text Policies** > **Unlock Text Policies**
Description	Configurable text for unlocking with a hybrid smart card when the computer is locked and `pid_unlock_option` is 1. **Note:** See `pid_unlock_text`.
Registry	
Type	String list
Values	To unlock, tap your hybrid smart card. If you do not have your hybrid smart card, click 'Unlock this computer'.
Scope	System
Note	• 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: Instructions for unlocking with hybrid smart card when the unlock policy is 'any user with or without current desktop account in Wallet can unlock'

IMS Entry	Instructions for unlocking with hybrid smart card when the unlock policy is 'any user with or without current desktop account in Wallet can unlock' (Maximum 2 lines)

pid_unlock_with_hsc_option_3_text: Instructions for unlocking with hybrid smart card when the 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, tap 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: 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'

IMS Entry	Instructions for unlocking with hybrid smart card when unlock policy is 'only the same user can unlock, but different user can re-log on to Windows' (Maximum 2 lines)
Location	**AccessAdmin** > **System** > **System policies** > **Configurable Text Policies** > **Unlock Text Policies**
Description	Configurable text for unlocking with a hybrid smart card when the computer is locked and `pid_unlock option` is 4. **Note:** See `pid_unlock_text`.
Registry	
Type	String list
Values	To unlock, tap your hybrid smart card. If you do not have your hybrid smart card, click 'Unlock this computer'.
Scope	System
Note	• 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: Instructions for unlocking with RFID when unlock policy is 'only the same user can unlock'

IMS Entry	Instructions for unlocking with RFID when unlock policy is 'only the same user can unlock' (Maximum 2 lines)

pid_unlock_with_rfid_option_1_text: Instructions for unlocking with RFID 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 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: Instructions for unlocking with RFID when unlock policy is 'any user with or without current desktop account in Wallet can unlock'

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: Instructions for unlocking with RFID when unlock policy is 'only the same user can unlock, but different user can re-log on to Windows'

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**

pid_unlock_with_rfid_option_4_text: Instructions for unlocking with RFID when unlock policy is 'only the same user can unlock, but different user can re-log on to Windows'

Description	Configurable text for unlocking with an RFID when the computer locked and `pid_unlock_option` is `4`. **Note:** See `pid_unlock_text`.
Registry	
Type	String list
Values	To unlock, tap your RFID card. If you do not have your RFID card, click 'Unlock this computer'.
Scope	System
Note	• 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: Instructions for unlocking with fingerprint when unlock policy is 'only the same user can unlock'

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: Instructions for unlocking with fingerprint when unlock policy is 'any user with or without current desktop account in Wallet can unlock'

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**

pid_unlock_with_fingerprint_option_3_text: Instructions for unlocking with fingerprint when unlock policy is 'any user with or without current desktop account in Wallet can unlock'

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: Instructions for unlocking with fingerprint when unlock policy is 'only the same user can unlock, but different user can re-log on to Windows'

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: Instructions for unlocking with fingerprint or RFID when unlock policy is 'only the same user can unlock'

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: Instructions for unlocking with fingerprint or RFID when unlock policy is 'only the same user can unlock'

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: Instructions for unlocking with fingerprint or RFID when unlock policy is 'any user with or without current desktop account in Wallet can unlock'

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: 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'

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**

pid_unlock_with_fingerprint_or_rfid_option_4_text: 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'

Description	Configurable text for unlocking with a fingerprint or an RFID when the computer is locked and `pid_unlock option` is `4`. **Note:** See `pid_unlock_text`.
Registry	
Type	String list
Values	To unlock, place your registered finger on the sensor or tap your RFID card. To unlock without fingerprint or RFID card, click 'Unlock this computer'.
Scope	System
Note	• 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: Template for sign-up dialog

IMS Entry	Template for sign-up dialog
Location	**AccessAdmin** > **System** > **System policies** > **Configurable Text Policies** > **Sign Up Text Policies**
Description	The template to be used for displaying the sign-up dialog. **Note:** 1. The **Domain** field is shown if the enterprise directory is the Active Directory. 2. Other than the domain, the template can support either one or two fields only. To display only one field, set the Label of one of the fields to a blank entry. The field with the blank Label is not displayed.
Registry	
Type	Bind template
Values	Enter your domain user name and password for identity verification. User name Password
Scope	System
Note	Refreshed on sync.

Accessibility policy

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

pid_accessibility_is_animation_enabled: Enable animation?

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	• #False: No • #True: Yes (default value)
Scope	Machine
Note	

Chapter 8. Policies for Private and Shared desktops

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

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

Shared workstation policies

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

Lock/Unlock Policies

pid_win_startup_action: Windows startup actions

IMS Entry	Windows startup actions
Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **Shared Workstation Policies** > **Lock/Unlock Policies**
Description	Actions on Windows startup. **Note:** Use this policy to enable automatic locking of the computer after **`AutoAdminLogon`** or **`ForceAutoLogon`**.
Registry	`[DO] "WinStartupAction"`
Type	DWORD
Values	• #0: No action (default value) • #1: Lock computer
Scope	Machine
Note	Refreshed on use.

pid_win_fast_user_switching_enabled: Enable support for Windows Fast User Switching?

IMS Entry	Enable support for Windows Fast User Switching?
Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **Shared Workstation Policies** > **Lock/Unlock Policies**
Description	Whether to enable support for Fast User Switching in Microsoft Windows 7 and later versions. **Note:** Effective only if the client operating system is Microsoft Windows 7 and later versions, and if Fast User Switching is enabled.
Registry	`[DO] "WinFastUserSwitchingEnabled"`
Type	Boolean
Values	• #True: Yes • #False: No (default value)
Scope	Machine

© Copyright IBM Corp. 2002, 2015

pid_win_fast_user_switching_enabled: Enable support for Windows Fast User Switching?

Note	• Refreshed on sync. • For Microsoft Windows 7 and Windows 8 only. • If set to **No**, the environment is similar to a personal desktop with one user. • If set to **Yes**, there are multiple sessions in the same desktop.

Chapter 9. Policies for Citrix and Terminal Server

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

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

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: TSLightweightMode

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.

© Copyright IBM Corp. 2002, 2015

Chapter 10. Policies for Debugging Management and Control

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

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: List of custom audit event codes and their corresponding display names

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

Troubleshooting policies

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

pid_wallet_sync_manual_enabled: WalletSyncManualEnabled

Location	**Registry Editor** > **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **IBM** > **ISAM ESSO** > **Temp**
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.

© Copyright IBM Corp. 2002, 2015

pid_wallet_delete_enabled: WalletDeleteEnabled

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 you delete the Wallets. If multiple sessions are running, the AccessAgent running in other sessions after deleting the Wallets might be unstable.
Registry	`[T] "WalletDeleteEnabled"`
Type	DWORD
Values	• #0: No (default value) • #1: Yes
Scope	Machine
Note	Refreshed on use.

pid_machine_policy_override_enabled: MachinePolicyOverrideEnabled

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"`
Type	DWORD
Values	• #0: No (default value) • #1: Yes
Scope	Machine
Note	Refreshed on use.

Temporary file policy

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

pid_temp_path: TempPath

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: LogFileCount

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: LogFileSize

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: LogLevel

Location	**Registry Editor** > **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **IBM** > **ISAM ESSO** > **DeploymentOptions**
Description	Level of log details.
Registry	`[DO] "LogLevel"`
Type	DWORD
Values	• #0: No logging • #1: Severe errors only (default value) • #2: Basic info • #3: More info, including SOAP logs • #4: Debugging info, including SOAP logs
Scope	Machine
Note	Refreshed on use.

pid_log_path: LogPath

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.

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: Enable 'Never' for enterprise authentication services?

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. If the user policy is defined, it overrides the system policy.
Registry	
Type	Boolean
Values	• #True: Yes (default value) • #False: No
Scope	User System
Note	Refreshed on sync.

pid_wallet_personal_app_sso_enabled: Enable single sign-on for personal authentication services?

IMS Entry	Enable single 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 single sign-on for personal authentication services.
Registry	
Type	Boolean
Values	• #True: Yes (default value) • #False: No
Scope	User System
Note	Refreshed on sync.

© Copyright IBM Corp. 2002, 2015

pid_accessagent_pwd_display_option: Option for displaying application passwords in AccessAgent

IMS Entry	Option for displaying application passwords in AccessAgent
Location	**AccessAdmin** > **User Policy Templates** > **New template** > **Create new policy template** > **Wallet Policies**
Description	Option for displaying application passwords in the Wallet Manager of AccessAgent through the **Show password** option. **Note:** 1. The user is asked to enter a password before the display of the application passwords. 2. Displaying application passwords is not enabled if the user is logged on using a fingerprint or smart card.
Registry	
Type	Non-negative integer
Values	• #0: Disallow displaying passwords. (default value) • #1: Allow displaying personal passwords. • #2: Allow displaying both enterprise and personal passwords.
Scope	User
Note	Refreshed on sync

pid_accessagent_pwd_export_option: Option for exporting application passwords in AccessAgent

IMS Entry	Option for exporting application passwords in AccessAgent
Location	**AccessAdmin** > **User Policy Templates** > **New template** > **Create new policy template** > **Wallet Policies**
Description	Option for exporting application passwords in the Wallet Manager of AccessAgent through the **Export?** option. **Note:** The user is asked to enter password before the user can export passwords.
Registry	
Type	Non-negative integer
Values	• #0: Disallow exporting passwords. (default value) • #1: Allow exporting personal passwords. • #2: Allow exporting both enterprise and personal passwords.
Scope	User
Note	Refreshed on sync.

pid_sso_user_control_enabled: Allow user to enable or not enable single sign-on?

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

pid_sso_user_control_enabled: Allow user to enable or not enable single sign-on?

Description	Whether to allow the user to enable or not enable single sign-on. **Note:** If this policy is not enabled, the **Enable single sign-on** and **Disable single sign-on** options do not display in the AccessAgent UI.
Registry	`[DO] "SsoUserControlEnabled"`
Type	DWORD Boolean
Values	• #True: Yes (default value) • #False: No
Scope	Machine User
Note	Refreshed on sync.

pid_wallet_editable_items_list: List of Wallet items that can be edited by the user through AccessAgent

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	• #1: Password • #2: Password entry option • #4: Application settings • #8: Delete credential • #16: Add credential
Scope	User
Note	

pid_wallet_cache_max: Maximum number of cached Wallets

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: Maximum number of cached Wallets

Description	Maximum number of cached Wallets that are 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 that logs on to the wrong Wallet. 4. Use this policy with `pid_wallet_cache_max_inactivity_days` so that the deleted cached Wallets can be automatically revoked on the IMS Server. 5. In some deployments, it might not be advisable to enable Wallet caching on shared workstations for security reasons. Set this policy to `0` so caching on a particular machine is not enabled. In this case, it overrides `pid_wallet_caching_option`.
Registry	`[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: Enable Wallet synchronization before logon?

IMS Entry	Enable Wallet synchronization before logon?
Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **Wallet Policies**
Description	Whether to enable AccessAgent to synchronize with the IMS Server before logon to the Wallet. **Note:** If this policy is set to 1, AccessAgent synchronizes with the IMS Server: • before logging on to Windows (for ESSO Credential Provider log on) • before running the logon script (for desktop logon and logon from an unlock screen)
Registry	`[DO] "WalletSyncBeforeLogonEnabled"`
Type	DWORD
Values	• #True: Yes (default value) • #False: No
Scope	Machine
Note	Refreshed on use.

pid_wallet_cache_security_enabled: Enable cached Wallet security?

IMS Entry	Enable cached Wallet security?

pid_wallet_cache_security_enabled: Enable cached Wallet security?

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 are created. The cached Wallets that are copied from another machine fail to work. 2. Do not enable this policy if cached Wallets are shared among several machines. For example, AccessAgent on Citrix servers might be configured to access the same network folder for storing cached Wallets. 3. This policy does not affect `pid_machine_policy_override_enabled`.
Registry	`[DO] "WalletCacheSecurityEnabled"`
Type	DWORD
Values	• #True: Yes • #False: No (default value)
Scope	Machine
Note	Refreshed on startup.

pid_wallet_caching_option: 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. If ESSO Network Provider is used, the Wallet is cached when this policy is set to `ask user` or `always cache`. 4. Wallet is always cached if a user logs on with a smart card, hybrid smart card, or fingerprint.
Registry	
Type	Non-negative integer
Values	• #0: Disallow caching • #1: Ask user (default value) • #2: Always cache
Scope	System, Machine
Note	Refreshed on sync.

pid_wallet_cache_max_inactivity_days: Maximum period of inactivity, in days, allowed for a cached Wallet

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: Maximum period of inactivity, in days, allowed for a cached Wallet

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 exceeded the maximum number of days for inactivity. AccessAgent automatically revokes expired cached Wallets during each periodic synchronization, and while a user is logged on to AccessAgent. 2. Inactivity is measured from the last synchronization time. Even if the user logs on to a cached Wallet every day, it can still be revoked. The cached Wallet is revoked if it is not synchronized with the IMS Server for an extended time. 3. If a cached Wallet is revoked, the user can log on only if the IMS Server is available. There must be no prompt that the Wallet is revoked. The option to cache the Wallet depends on `pid_wallet_caching_option`.
Registry	
Type	Positive integer
Values	999999999 (default value)
Scope	System
Note	• Set to 999999999 for infinity; cached Wallets do not expire. • Refreshed on sync.

pid_wallet_sync_mins: Interval, in minutes, for the Wallet synchronization with the IMS Server

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

pid_wallet_open_max_tries: Maximum number of consecutive invalid offline logons before the cached Wallet is locked out

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

pid_wallet_open_max_tries: Maximum number of consecutive invalid offline logons before the cached Wallet is locked out

Values	5 (default value)
Scope	System
Note	Refreshed on sync.

pid_wallet_inject_pwd_entry_option_default: Default single sign-on password entry option

IMS Entry	Default single sign-on password entry option
Location	**AccessAdmin** > **System** > **System policies** > **Wallet Policies**
Description	Default single sign-on password entry option.
Registry	
Type	Positive integer
Values	• #1: Automatic log on • #2: Always (default value) • #3: Ask • #4: Never
Scope	System
Note	Refreshed on sync.

pid_sso_auto_learn_enabled: Enable auto-learning?

IMS Entry	Enable auto-learning?
Location	**AccessAdmin** > **System** > **System policies** > **Wallet Policies**
Description	Whether auto-learning can be enabled for single sign-on to applications.
Registry	
Type	Boolean
Values	• #True: Yes (default value) • #False: No
Scope	System
Note	Refreshed on sync.

pid_migration_stage: Stage of migration from version 1.x to 3.x

IMS Entry	Stage of migration from version 1.x to 3.x
Location	**AccessAdmin** > **System** > **System policies** > **Wallet Policies**

pid_migration_stage: Stage of migration from version 1.x to 3.x

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 are upgraded. 4. The Wallets are upgraded as and when the user logs on using the upgraded AccessAgent. After all Wallets are upgraded, the policy must be set to 0 to optimize the IMS Server and AccessAgent performance.
Registry	
Type	Non-negative integer
Values	• #0: No migration or migration completed. (default value) • #1: Upgrading ISAM ESSO IMS Server and AccessAgent. • #2: ISAM ESSO IMS Server and AccessAgent fully upgraded.
Scope	System
Note	Refreshed on sync.

pid_wallet_cleanup_on_caching_enabled: WalletCleanupOnCachingEnabled

IMS Entry	
Location	**Registry Editor** > **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **IBM** > **ISAM ESSO** > **DeploymentOptions**
Description	Whether to do 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 run cleanup.
Registry	[DO] "WalletCleanupOnCachingEnabled"
Type	DWORD
Values	• #0: disabled • #1: enabled
Scope	Machine
Note	

AccessAgent policies

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

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: Enable bubble pop-ups?

IMS Entry	Enable bubble pop-ups?
Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **Display Policies**
Description	Whether to enable the bubble pop-up notification of AccessAgent at the Windows notification area.
Registry	`[DO] "AATrayBubbleDisplayEnabled"`
Type	Boolean DWORD
Values	• #True: Yes (default value) • #False: No
Scope	Machine
Note	Refreshed on use.

pid_aa_tray_menu_options_enabled: Enable right-click menu options?

IMS Entry	Enable right-click menu options?
Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **Display Policies**
Description	Whether to display menu options when the user right-clicks the AccessAgent icon at the Windows notification area.
Registry	
Type	
Values	• #True: Yes (default value) • #False: No
Scope	Machine
Note	

pid_session_info_display_freq_secs: Interval, in seconds, for displaying session information in bubble pop-ups

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**

pid_session_info_display_freq_secs: Interval, in seconds, for displaying session information in bubble pop-ups

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 computer 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: AccessAgent Feedback link

IMS Entry	AccessAgent Feedback link
Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **Display Policies**
Description	Enables the **Feedback** link in the AccessAgent user interface, which launches an email client or web browser. **Note:** • If the policy value is blank, (default) AccessAgent does not show the **Feedback** link. • If the policy value format is `mailto:abc@example.com`, clicking **Feedback** launches the default email client of the user and the email is sent to `abc@example.com`. • If the policy value format is `http://example.com`, clicking **Feedback** launches the default browser of the user and navigates to `http://example.com`.
Registry	`[DO] "AAFeedbackLink"`
Type	String SZ
Values	
Scope	Machine
Note	Refreshed on sync.

pid_ims_server_name: ImsServerName

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

ESSO Credential Provider policies

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

pid_engina_winlogon_option_enabled: Allow logon bypass through Windows?

IMS Entry	Allow logon bypass through Windows?
Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **ESSO Credential Provider Policies**
Description	Whether to enable the option to go to Windows Logon directly from ESSO Credential Provider.
Registry	`[DO] "EnginaWinlogonOptionEnabled"`
Type	DWORD
Values	• #1: Yes (default value) • #0: No
Scope	Machine
Note	Refreshed on use.

pid_engina_app_launch_enabled: Enable application launch from ESSO Credential Provider?

IMS Entry	Enable application launch from ESSO Credential Provider?
Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **ESSO Credential Provider Policies**
Description	Whether to enable the launching of an application from the ESSO Credential Provider welcome or locked screen. **Note:** This policy is not supported when Transparent Screen Lock is enabled.
Registry	`[DO] "EnginaAppLaunchEnabled"`
Type	DWORD
Values	• #1: Yes • #0: No (default value)
Scope	Machine
Note	Refreshed on use.

pid_engina_app_launch_label: Display label for application launch

IMS Entry	Display label for application launch
Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **ESSO Credential Provider Policies**
Description	Display label for the link on ESSO Credential Provider welcome or locked screen, for launching an application. **Note:** • Effective only if `pid_engina_app_launch_enabled` is 1. • This policy is not supported when Transparent Screen Lock is enabled.
Registry	`[DO] "EnginaAppLaunchLabel"`
Type	SZ
Values	
Scope	Machine
Note	Refreshed on use.

pid_engina_app_launch_cmd: Command line for application launch

IMS Entry	Command line for application launch
Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **ESSO Credential Provider Policies**
Description	Command line for launching an application from an ESSO Credential Provider 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**. 4. This policy is not supported when Transparent Screen Lock is enabled.
Registry	`[DO] "EnginaAppLaunchCmd"`
Type	SZ
Values	
Scope	Machine
Note	Refreshed on use.

pid_engina_bypass_hot_key_enabled: Enable ESSO Credential Provider Bypass Hot Key?

IMS Entry	Enable ESSO Credential Provider Bypass Hot Key?
Location	• **AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **ESSO Credential Provider Policies** • **AccessAdmin** > **System** > **System policies** > **AccessAgent Policies** > **ESSO Credential Provider Policies**

pid_engina_bypass_hot_key_enabled: Enable ESSO Credential Provider Bypass Hot Key?

Description	Whether the ESSO Credential Provider Bypass Hot Key is enabled. **Note:** 1. If enabled, the user can press the ESSO Credential Provider Bypass Hot Key sequence to bypass ESSO Credential Provider and go to Windows to log on or unlock. 2. The Hot Key is accepted at any of the following ESSO Credential Provider 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 Credential Provider 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	• #1: Yes (default value) • #0: No • #1: True (default value) • #0: False
Scope	Machine System
Note	Refreshed on startup.

pid_engina_bypass_hot_key_sequence: ESSO Credential Provider Bypass Hot Key sequence

IMS Entry	ESSO Credential Provider Bypass Hot Key sequence
Location	• **AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **ESSO Credential Provider Policies** • **AccessAdmin** > **System** > **System policies** > **AccessAgent Policies** > **ESSO Credential Provider Policies**
Description	The ESSO Credential Provider Bypass Hot Key sequence. Maximum of 3 keys from the set: {Ctrl, Shift, Alt, Ins, Del, Home, End, PgUp, PgDn, Break, E}. **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"`

pid_engina_bypass_hot_key_sequence: ESSO Credential Provider Bypass Hot Key sequence

Type	MULTI_SZ String list
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: Enable automatic ESSO Credential Provider bypass?

IMS Entry	Enable automatic ESSO Credential Provider bypass?
Location	**AccessAdmin > Machine Policy Templates > New template > Create new machine policy template > AccessAgent Policies > ESSO Credential Provider Policies**

pid_engina_bypass_automatic_enabled: Enable automatic ESSO Credential Provider bypass?

Description	Whether automatic ESSO Credential Provider 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 ESSO Credential Provider. Microsoft Credential Provider 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 Credential Provider 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"`
Type	DWORD
Values	• #1: Yes • #0: 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: Desktop inactivity duration, in minutes

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 can do a set of actions.
Registry	`[DO] "DesktopInactivityMins"`
Type	DWORD Positive integer
Values	30 (default value)

pid_desktop_inactivity_mins: Desktop inactivity duration, in minutes

Scope	Machine System
Note	• Refreshed on sync for system policy. • Refreshed on use for machine policy.

pid_desktop_inactivity_action: Desktop inactivity actions

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**
Description	Actions to be done 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	• #0: No action (default value) • #1: Log off Windows • #2: Log off Wallet • #4: Lock computer • #5: Log off Wallet and lock computer
Scope	Machine System
Note	• Refreshed on sync for system policy. • Refreshed on use for machine policy.

pid_desktop_inactivity_action_countdown_secs: Confirmation countdown duration, in seconds, for desktop inactivity

IMS Entry	Confirmation countdown duration, in seconds, for desktop inactivity

pid_desktop_inactivity_action_countdown_secs: 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. Set the value to 0 to disable confirmation countdown.
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: Actions on Windows screen saver activation

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 done 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 7 or later.
Registry	`[DO] "WinScreensaverAction"`

pid_win_screensaver_action: Actions on Windows screen saver activation

Type	DWORD Non-negative integer
Values	• #0: Disable Windows screen saver • #1: If screen saver is password protected, lock computer, else show normal screen saver • #2: Lock computer (default value)
Scope	Machine System
Note	• Refreshed on sync for system policy. • Refreshed on use for machine policy. AccessAgent assumes that `ScreenSaverGracePeriod` is 0 when it locks the computer and screen saver activation. If the user dismisses the screensaver before the grace period is over, the computer remains unlocked, but the lock scripts are run.

pid_locked_computer_inactivity_mins: Locked computer inactivity duration, in minutes

IMS Entry	Locked computer 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	Locked computer inactivity duration, in minutes, after which AccessAgent can 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: Locked computer inactivity actions when the user is logged on to the Wallet

IMS Entry	Locked computer inactivity actions when the user is logged on to the Wallet

pid_locked_computer_inactivity_action: Locked computer inactivity actions when the user is logged on to the 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	Actions to be done by AccessAgent after a period of desktop inactivity while the computer is locked and the user is logged on to the Wallet. **Note:** 1. Effective only if `pid_lusm_sessions_max` is 1. 2. This policy is effective only if the ESSO Credential Provider screen lock is shown.
Registry	`[DO] "LockedComputerInactivityAction"`
Type	DWORD Non-negative integer
Values	• #0: No action (default value) • #1: Log off Windows
Scope	Machine System
Note	• Refreshed on sync for system policy. • Refreshed on use for machine policy.

Lock and Unlock policies

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

pid_script_lock_enabled: Enable lock script during locking of the user's AccessAgent session

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

pid_script_lock_enabled: Enable lock script during locking of the user's AccessAgent session

Description	Whether to enable running the lock script when locking the AccessAgent session of the user. **Note:** 1. The lock script is run only if the session of the user is visible during locking. In Local User Session Management (LUSM), currently invisible user sessions do not have the lock script executed. 2. The lock script is run regardless of whether there is desktop inactivity or locking is manually triggered. For example, pressing Win+L or tapping an RFID card. 3. The lock script is useful for closing applications when locking a guest AccessAgent session. The lock script can also be used with the unlock script in a Local User Session Management scenario to record any single-instance application that might: • be running before lock. • be relaunched during unlock. **Important:** When using Microsoft Windows 7 or later: • The lock script is run after the computer locks instead of before the computer locks. • The user is not prompted for action upon computer lock. Blocking lock scripts are not supported. The scripts are expected to perform non-blocking actions. For instance, a message box prompt in the script is not supported.
Registry	
Type	Boolean
Values	• #True: Yes • #False: No (default value)
Scope	User
Note	Refreshed on sync.

pid_script_lock_type: Lock script 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	• #1: Batch (default) • #2: VBScript
Scope	User

pid_script_lock_type: Lock script type

Note	Refreshed on sync.

pid_script_lock_code: Lock script 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: Enable unlock script when user unlocks an existing AccessAgent session?

IMS Entry	Enable unlock script when user unlocks an existing AccessAgent session?
Location	**AccessAdmin** > **User Policy Templates** > **New template** > **Create new policy template** > **AccessAgent Policies** > **Lock/Unlock Policies**
Description	Whether to enable the running of the unlock script when the user unlocks an existing AccessAgent session. **Note:** 1. The unlock script is run only if the user has an existing AccessAgent session and is unlocking the session. 2. The unlock script is not run if the user is unlocking a shared workstation that is: • logged on with a generic Windows account and • not currently logged on to AccessAgent In this case, the logon script (`pid_script_logon_enabled`) is run instead. 3. The unlock script can be used in Local User Session Management. The script can automatically launch single-instance applications that might be terminated by other users who are logged on to the same workstation. 4. The unlock script is not supported if `pid_lock_option` is `2` (such as transparent screen lock is used).
Registry	
Type	Boolean
Values	• #True: Yes • #False: No (default value)
Scope	User
Note	Refreshed on sync.

pid_script_unlock_type: Unlock script 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	• #1: Batch (default) • #2: VBScript
Scope	User
Note	Refreshed on sync.

pid_script_unlock_code: Unlock script 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: Unlock computer policy

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: Unlock computer policy

Description	Unlock computer policy for controlling who can unlock a computer when it is locked by a user who is logged on to AccessAgent. Same user refers to the same user who locked the computer. Administrator refers to the Windows user with Administrator privilege on that computer. The Wallet must contain the Windows credentials of an Administrator user on that computer. **Note:** 1. Effective only if `pid_lusm_sessions_max` is `1`. 2. This policy is ignored if `pid_lock_option` is `2` (transparent screen lock). In transparent screen lock mode, any user can unlock the computer. 3. If the policy is set to `3` and a different user tries to unlock the computer, AccessAgent unlocks the computer and displays the current desktop. However, AccessAgent logs on the user to a new Wallet. 4. If the policy is set to `4`, only the same user can unlock the computer and return to the current desktop. For other users, AccessAgent logs off from the old desktop and logs on to the new Wallet. AccessAgent does not require a user to present a second factor. If a new Wallet does not have a desktop account on the computer, the user must log on to Windows. This option is not supported for smart card. **Important:** Limitations for Microsoft Windows 7 or later versions: • Option `3` works only with a Shared Desktop. • Option `4` logs off the current AccessAgent logon session without attempting to log on again as a second user.
Registry	`[DO] "UnlockOption"`
Type	DWORD Positive integer
Values	• #1: Only the same user can unlock • #3: Any user with or without current desktop account Wallet can unlock (default value) • #4: Only the same user can unlock, but different user can re-log on to Windows
Scope	Machine User
Note	• Refreshed on sync for user policy. • Refreshed on use for machine policy.

pid_unlock_different_user_action_countdown_secs: Confirmation countdown duration, in seconds, for unlocking by a different user

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: Confirmation countdown duration, in seconds, for unlocking by a different user

Description	Confirmation countdown duration, in seconds, for unlocking by a different user. Set the value to 0 to disable confirmation countdown **Note:** 1. Effective only if `pid_lusm_sessions_max` is 2. 2. Effective when a user attempts to unlock a computer when another user is already logged on to AccessAgent. 3. If the policy value is not `0`, the user can click the prompt to cancel the switch user. If the user does not confirm, AccessAgent proceeds to unlock the computer.
Registry	`[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: Screen 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 (ESSO Credential Provider screen lock) is supported. 2. From a transparent screen lock, the user can unlock the computer or switch to another user by presenting a second factor. 3. From a transparent screen lock, the AccessAgent UI is displayed when the IBM Security Access Manager for Enterprise Single Sign-On Hot Key is pressed. From this screen, the user can manually log off from AccessAgent, which unlocks the computer, and does the actions that are specified by `pid_logoff_manual_action`. The logoff action is available regardless of the setting for `pid_logoff_manual_when_locked_option_enabled`. 4. Even after transparent screen lock is activated, the action that is specified by `pid_desktop_inactivity_action` is still carried out after the period of desktop inactivity elapsed. Then, set `pid_desktop_inactivity_action` to `4`.
Registry	`[DO] "LockOption"`
Type	DWORD
Values	• #1: ESSO Credential Provider screen lock (default) • #2: Transparent screen lock
Scope	Machine
Note	Refreshed on use.

pid_lock_transparent_text: Transparent screen lock message

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: Enable transparent screen lock hot key?

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	• #1: Yes • #0: No (default value)
Scope	Machine
Note	Refreshed on use.

pid_unlock_with_win_option: Option for allowing unlock bypass through Windows

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: Option for allowing unlock bypass through Windows

Description	Option for unlocking the computer with 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 with 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: User name prefill option for unlock prompt

IMS Entry	User name prefill option for unlock prompt
Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **Lock/Unlock Policies**
Description	Option for pre-filling the AccessAgent unlock prompt with a user name. • For policy value 0, the setting for pid_logon_user_name_prefill_option applies to the unlock prompt. • For policy value 1, if a user is logged on to AccessAgent, the unlock prompt is pre-filled with the currently logged on user name. If no user is logged on to AccessAgent, the unlock prompt is pre-filled with last logged on user name. • This policy is not applicable to private desktop (pid_lusm_sessions_max is greater than 1).
Registry	[DO] "UnlockUserNamePrefillOption"
Type	DWORD
Values	• #0: Use the user name pre-fill option for logon prompt (default value) • #1: Prefill with currently logged on or last logged on user name
Scope	Machine
Note	Refreshed on use.

pid_fast_unlock_enabled: Enable fast unlock without IMS Server check?

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

pid_fast_unlock_enabled: Enable fast unlock without IMS Server check?

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: Smart card removal actions

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 done when a smart card is removed.
Registry	
Type	Non-negative integer
Values	• #1: Log off Windows • #2: Log off Wallet • #4: Lock computer (default value) • #5: Log off Wallet and lock computer
Scope	Machine User
Note	

pid_sc_win_logon_enabled: Enable Windows smart card logon?

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 through 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 with the smart card certificate. 2. This policy is only applicable if the `pid_engina_ui_enabled` policy is set. This policy is not supported on Windows 7 or later versions.
Registry	
Type	Boolean
Values	• #True: Yes • #False: No (default value)

pid_sc_win_logon_enabled: Enable Windows smart card logon?

Scope	Machine
Note	Refreshed on sync.

pid_sc_map_cert_to_entdir_acc_enabled: Enable automatic mapping of certificate to the enterprise directory account during sign up?

IMS Entry	Enable automatic mapping of certificate to the enterprise directory account during sign up?
Location	**AccessAdmin** > **System** > **System policies** > **AccessAgent Policies** > **Smart card Policies**
Description	Whether to automatically identify the enterprise directory account by using the smart card certificate attributes during sign-up. The user is not prompted to provide a user name during sign-up.
Registry	
Type	Boolean
Values	• #True: Yes • #False: No (default value)
Scope	System
Note	Refreshed on sync.

pid_engina_ui_enabled: Enable the ISAM ESSO UI when Windows is logged off or locked?

IMS Entry	Enable the ISAM ESSO UI when Windows is logged off or locked?
Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **Smart card Policies**
Description	Whether to display the IBM Security Access Manager for Enterprise Single Sign-On UI instead of the Windows UI when Windows is logged off or locked.
Registry	
Type	Boolean
Values	• #True: Yes (default value) • #False: No
Scope	Machine
Note	Refreshed on sync.

Hybrid smart card policies

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

pid_sc_1f_unlock_enabled: Enable single factor smart card unlock?

IMS Entry	Enable single factor smart card unlock?

pid_sc_1f_unlock_enabled: Enable 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	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: Yes • #False: No (default value)
Scope	Machine User
Note	

pid_sc_1f_unlock_timeout_secs: Time expiry, in seconds, for single factor smart card unlock

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: Enable single factor smart card logon?

IMS Entry	Enable single factor smart card logon?
Location	**AccessAdmin** > **Machine Policy Templates** > **New Template** > **AccessAgent Policies** > **Smart card Policies**
Description	Whether to allow a single factor smart card logon without a PIN by a user who recently logged on using smart card and PIN on the same computer or another computer. This policy applies if logon happens in the duration that is specified by the single factor smart card logon timeout.
Registry	
Type	Boolean

pid_sc_1f_logon_enable: Enable single factor smart card logon?

Values	• #True: Yes • #False: No (default value)
Scope	Machine
Note	

pid_sc_1f_logon_timeout_mins: Time expiry, in minutes, for single factor smart card logon

IMS Entry	Time expiry, in minutes, for single factor smart card logon
Location	**AccessAdmin** > **User Policy Template** > **New Template** > **AccessAgent Policies** > **Smart card Policies**
Description	Time expiry, in minutes, for single factor smart card logon. After this duration (timed from last logon with smart card and PIN), single factor smart card logon is not allowed.
Registry	
Type	Non-negative integer
Values	• >0: Grace period in minutes • 0: Invalid. Single factor smart card logon is Not enabled.
Scope	User
Note	

pid_sc_1f_logon_extension_allowed: Extend single factor smart card logon time expiry when user logs on with smart card and PIN?

IMS Entry	Extend single factor smart card logon time expiry when user logs on with smart card and PIN?
Location	**AccessAdmin** > **User Policy Template** > **New Template** > **AccessAgent Policies** > **Smart card Policies**
Description	Whether to extend the time expiry for single factor smart card logon when the user logs on with a smart card and PIN before grace period expires.
Registry	
Type	
Values	• No • Yes
Scope	Machine User
Note	

pid_sc_present_same_action: Actions on the desktop for using the same smart card if user logged on with single factor

IMS Entry	Actions on the desktop for using the same smart card if user logged on with single factor

pid_sc_present_same_action: Actions on the desktop for using the same smart card if user logged on with single factor

Location	**AccessAdmin** > **Machine Policy Templates** > **New Template** > **AccessAgent Policies** > **Smart card PoliciesAccessAdmin** > **User Policy Template** > **New Template** > **AccessAgent Policies** > **Smart card Policies**
Description	Actions on the desktop for using the same smart card. This policy is effective only if the current user session starts with a single factor smart card logon.
Registry	
Type	Non-negative integer
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: Confirmation countdown duration, in seconds, on the desktop, for using the same smart card

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

pid_sc_present_different_action: Actions on the desktop for using a different smart card if the user logged on with single factor

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

pid_sc_present_different_action: Actions on the desktop for using a different smart card if the user logged on with single factor

Description	Actions on the desktop for using a different smart card. This policy is effective only if the current user session starts with a single factor smart card logon.
Registry	
Type	Non-negative integer
Values	• #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: Confirmation countdown duration, in seconds, on the desktop, for using a different smart card

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

IMS Entry	Actions on the desktop for tapping same RFID

pid_rfid_tap_same_action: Actions on the desktop for tapping same RFID

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 done by AccessAgent on the desktop when the currently logged on user taps his RFID card **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	• #0: No action (default value) • #1: Log off Windows • #2: Log off Wallet • #4: Lock computer • #5: Log off Wallet and lock computer
Scope	Machine User
Note	• Refreshed on sync for user policy. • Refreshed on use for machine policy.

pid_rfid_tap_same_action_countdown_secs: Confirmation countdown duration in seconds, on the desktop, for tapping same RFID on the card reader

IMS Entry	Confirmation countdown duration in seconds, on the desktop, for tapping same RFID on the card reader
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, on the desktop, for tapping same RFID on the card reader. Set the value to 0 to disable confirmation countdown.
Registry	`[DO] "RfidTapSameActionCountdownSecs"`
Type	DWORD Non-negative integer
Values	5 (default value)
Scope	Machine User

pid_rfid_tap_same_action_countdown_secs: Confirmation countdown duration in seconds, on the desktop, for tapping same RFID on the card reader

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: Enable RFID-only unlock?

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.
Registry	`[DO] "RfidOnlyUnlockEnabled"`
Type	DWORD Boolean
Values	• #1: Yes • #0: 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: Time expiry, in seconds, for RFID-only unlock

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)

pid_rfid_only_unlock_timeout_secs: Time expiry, in seconds, for RFID-only unlock

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: Time expiry, in minutes, for RFID-only logon

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: Actions on the desktop for tapping different RFID

IMS Entry	Actions on the desktop for tapping different RFID
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_different_action: Actions on the desktop for tapping different RFID

Description	Actions to be done by AccessAgent on the desktop when an RFID card that does not belong to the currently logged on user is tapped on the card reader. **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 logoff from Windows. 4. If `pid_lusm_sessions_max` is greater than `1`, AccessAgent with a policy value of `1` (Log off Windows) logs off the desktop session of the user. The computer locked screen is displayed. AccessAgent with a policy value of `6` (Switch user) attempts to create a user desktop session for the new user. AccessAgent with a policy value of `8` (Log off Windows and log on as a new user) logs off the desktop session of the current user and creates a user desktop session for the new user. 5. Switching of a user is only supported for users who use the same type of second factor. 6. If `pid_rfid_tap_different_action` has the value of `Switch user`, and `pid_win_fast_user_switching_enabled` is enabled, fast user switching takes place. **Important:** Limitation for Microsoft Windows Windows 7 or later versions: For the value **Log off Windows and log on as new user**, AccessAgent logs off the current logon session without attempting to log on again as a second user.
Registry	`[DO] "RfidTapDifferentAction"`
Type	DWORD Non-negative integer
Values	• #0: No action (default value) • #4: Lock computer • #5: Log off Wallet and lock computer • #6: Switch user • #8: Log off Windows and log on as new user
Scope	Machine User
Note	• Refreshed on sync for user policy. • Refreshed on use for machine policy.

pid_rfid_tap_different_action_countdown_secs: Confirmation countdown duration in seconds, on the desktop, for tapping different RFID on the card reader

IMS Entry	Confirmation countdown duration in seconds, on the desktop, for tapping different RFID on the card reader

pid_rfid_tap_different_action_countdown_secs: Confirmation countdown duration in seconds, on the desktop, for tapping different RFID on the card reader

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, on the desktop, for tapping different RFID on the card reader. Set the value to 0 to disable confirmation countdown.
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: Enable RFID-only logon?

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: Enable RFID-only logon?

Description	Whether to allow RFID-only logon (without password) by a user who recently logged on using an RFID and password on the same or another computer, if logon happens within the duration that is specified by the RFID-only logon time-out (`pid_rfid_only_logon_timeout_mins`) **Note:** 1. RFID-only logon works only if the IMS Server is online and the user has an existing cached Wallet on the computer. 2. RFID-only logon is tied to the specific RFID card used for logon. If the user has two RFID cards, and the first card is logged on, the user can log on only with the first RFID card. If the user attempts to log on with the second RFID card, the user must be prompted for a password. 3. For better security, `pid_wallet_cache_max_inactivity_days` must be set to clear inactive Wallets. 4. RFID-only logon is not supported if `pid_lusm_sessions_max` is greater than 1. 5. ARFID is not applicable. 6. Either condition is applicable if both RFID-only unlock and RFID-only logon features are enabled: • 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 triggered. If the RFID-only unlock timeout has expired, the RFID-only logon is triggered. Ithe RFID-only unlock timeout has also expired, a password is required. • 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	• #1: Yes • #0: No (default value)
Scope	Machine
Note	Refreshed on use.

pid_rfid_display_utility_enabled: Enable RFID display utility?

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 works only when a user is logged on to AccessAgent.
Registry	`[DO] "RfidDisplayUtilityEnabled"`
Type	DWORD

pid_rfid_display_utility_enabled: Enable RFID display utility?

Values	• #1: Yes • #0: No (default value)
Scope	Machine
Note	Refreshed on use.

Fingerprint policies

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

pid_fingerprint_tap_same_action: Actions on the desktop for tapping the same finger

IMS Entry	Actions on the desktop for tapping the same finger
Location	• **AccessAdmin** > **User Policy Templates** > **AccessAgent Policies** > **Fingerprint Policies** • **AccessAdmin** > **Machine Policy Templates** > **AccessAgent Policies** > **Fingerprint Policies**
Description	Actions to be done by AccessAgent on the desktop when the currently logged on user taps a finger on the fingerprint 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	• #0: No action (default value) • #1: Log off Windows • #2: Log off Wallet • #4: Lock computer • #5: Log off Wallet and lock computer
Scope	Machine User
Note	• Refreshed on sync for user policy. • Refreshed on use for machine policy.

pid_fingerprint_tap_same_action_countdown_secs: Confirmation countdown duration, in seconds, on the desktop, for tapping the same finger on the fingerprint reader

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

pid_fingerprint_tap_same_action_countdown_secs: Confirmation countdown duration, in seconds, on the desktop, for tapping the same finger on the fingerprint reader

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, on the desktop, for tapping the same finger on the fingerprint reader. Set the value to 0 to disable confirmation countdown.
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: Actions on the desktop for tapping a different finger

IMS Entry	Actions on the desktop for tapping a different finger
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**

pid_fingerprint_tap_different_action: Actions on the desktop for tapping a different finger

Description	Actions to be done by AccessAgent on the desktop when a finger that does not belong to the currently logged on user is tapped on the fingerprint reader. **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 log off from Windows. 3. This policy is supported only if `pid_lusm_sessions_max` is 1. If `pid_lusm_sessions_max` is set to greater than 1, AccessAgent with a policy value 1 (Log off Windows) logs off the user from the desktop session. The computer locked screen is displayed. AccessAgent with a policy value of 6 (Switch user) attempts to create a user desktop session for the new user. AccessAgent with a policy value of 8 (Log off Windows and log on as new user) logs off the current user from the desktop session and creates a user desktop session for the new user. **Important:** Limitation for Microsoft Windows 7 or later versions: For option 8, AccessAgent logs off the current logon session without attempting to log on again as a second user.
Registry	`[DO] "FingerprintTap DifferentAction"`
Type	DWORD Non-negative integer
Values	• #0: No action (default value) • #4: Lock computer • #5: Log off Wallet and lock computer • #6: Switch user • #8: Log off Windows and log on as new user
Scope	Machine User
Note	• Refreshed on sync for user policy. • Refreshed on use for machine policy.

pid_fingerprint_tap_different_action_countdown_secs: Confirmation countdown duration, in seconds, on the desktop, for tapping a different finger on the fingerprint reader

IMS Entry	Confirmation countdown duration, in seconds, on the desktop, for tapping a different finger on the fingerprint reader
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, on the desktop, for tapping a different finger on the fingerprint reader. Set the value to 0 to disable confirmation countdown.

pid_fingerprint_tap_different_action_countdown_secs: Confirmation countdown duration, in seconds, on the desktop, for tapping 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: Maximum number of fingerprints that can be registered per user

IMS Entry	Maximum number of fingerprints that can be registered per user
Location	**AccessAdmin** > **System** > **System policies** > **AccessAgent Policies** > **Fingerprint Policies**
Description	Maximum number of fingerprints that each user is allowed to register. **Note:** A user who exceeded the maximum number of registered fingerprints can log on with any of the registered fingerprints if the value of this policy is reduced. However, to register a new fingerprint, an existing fingerprint has to be replaced. The user cannot increase the number of registered fingerprints.
Registry	
Type	Positive integer
Values	1 (default)
Scope	System
Note	• You can specify a minimum of one registered fingerprint, and a maximum of 10 registered fingerprints. • Refreshed on sync.

pid_fast_logon_enabled: Enable fast logon using cached Wallet without authenticating with the IMS Server?

IMS Entry	Enable fast logon using cached Wallet without authenticating with the IMS Server?
Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **Fingerprint Policies**

pid_fast_logon_enabled: Enable fast logon using cached Wallet without authenticating with the IMS Server?

Description	Users with cached Wallets can log on to AccessAgent without authenticating with the IMS Server. The fingerprint that is used to log on is validated against the IMS Server after AccessAgent connects to the desktop. To do authentication after logon, enable background authentication.
Registry	
Type	Positive integer
Values	• 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 is revoked, the user is logged off from the session. • If `pid_fast_logon_enabled` is set to `Yes`, and `pid_background_auth_enabled` is set to 0, AccessAgent does not check with the IMS Server for the validity of the scanned fingerprint. A user can still log on to the Windows desktop with a revoked fingerprint.

Terminal Server policies

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

pid_ts_logon_prompt_enabled: Enable auto-launching of AccessAgent log on prompt?

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**
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	• #1: Yes • #0: No (default value)
Scope	Machine
Note	Refreshed on use.

pid_ts_engina_logon_no_local_session_enabled: Use ESSO Credential Provider log on when there is no local AccessAgent session?

IMS Entry	Use ESSO Credential Provider log on when there is no local AccessAgent session?

pid_ts_engina_logon_no_local_session_enabled: Use ESSO Credential Provider log on when there is no local AccessAgent session?

Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **Terminal Server Policies**
Description	Whether to use ESSO Credential Provider logon or Microsoft Credential Provider 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	• #1: Yes • #0: No (default value)
Scope	Machine
Note	Refreshed on use.

pid_ts_aa_menu_option: Option for displaying menu options on the remote AccessAgent

IMS Entry	Option for displaying menu options on the remote AccessAgent
Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **Terminal Server Policies**
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: Enable COM port redirection?

IMS Entry	Enable COM port redirection?
Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **Terminal Server Policies**
Description	Whether the device monitoring mechanism can do a COM port redirection from the client machine (connecting to the Terminal Server) to the Terminal Server. **Note:** 1. If redirection is enabled for AccessAgent on Terminal Server or Citrix server, authentication devices on remote client machines can be monitored. For example, thin clients with no AccessAgent installed can be monitored.AccessAgent maps a virtual COM port (`pid_com_redir_local_virtual_port`) on the Terminal Server or Citrix server to a physical COM port (`pid_com_redir_remote_physical_port`) on the remote client. 2. Modifying this policy requires a computer restart to implement the changes.
Registry	`[DO] "ComRedirEnabled"`
Type	DWORD
Values	• #1: Yes • #0: No (default value)
Scope	Machine
Note	Refreshed on startup.

pid_com_redir_local_virtual_port: Virtual COM port on the Terminal Server

IMS Entry	Virtual COM port on the Terminal Server
Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **Terminal Server Policies**
Description	Virtual COM port on the Terminal Server to which data from the client COM port is redirected. **Note:** Effective only if `pid_com_redir_enabled` is 1.
Registry	`[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: Physical COM port on the client machine

IMS Entry	Physical COM port on the client machine
Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **Terminal Server Policies**

pid_com_redir_remote_physical_port: Physical COM port on the client machine

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 computer 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: TSStartAANoLocalAAEnabled

Location	**Registry Editor** > **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **IBM** > **ISAM ESSO** > **DeploymentOptions**
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 applies to launching of published applications only. If a remote desktop is launched, the remote AccessAgent is always started. 3. For a policy value of `0`, users cannot log on to a remote AccessAgent from computers that do not have a local AccessAgent installed (for example, home or Internet café).
Registry	`[DO] "TSStartAANoLocalAAEnabled"`
Type	DWORD
Values	• #1: Yes (default value) • #0: No
Scope	Machine
Note	Refreshed on use.

pid_machine_type_ts: MachineTypeTS

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

pid_machine_type_ts: MachineTypeTS

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 log on to remote AccessAgent uses credentials that are submitted by local AccessAgent. • It uses a Terminal Service second factor bypass option to determine its behavior when the authentication policy of the user requires a second factor for logon. 3. The following combinations of policy settings are not supported (behavior is unpredictable): • policy value `0` on a Terminal Server or Citrix server installation. • policy value `1` on a client machine installation. Modifying this policy requires a computer restart to implement the changes.
Registry	`[DO] "MachineTypeTS"`
Type	DWORD
Values	• #1: Machine is Terminal Server • #0: Machine is not Terminal Server (default value)
Scope	Machine
Note	Refreshed on startup.

pid_ts_delay_app_launch_exe_list: TSDelayAppLaunchExeList

Location	**Registry Editor** > **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **IBM** > **ISAM ESSO** > **ECSS** > **DeploymentOptions**
Description	The list of applications which are delayed from launching until the remote AccessAgent is ready to do single 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: TSDelayAppLaunchEnabled

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 through RDP. 2. This policy must be set on the remote AccessAgent, such as on the Citrix server. 3. If not enabled, the user might first see the logon prompt of the application before the remote AccessAgent can do single sign-on. This result might cause some confusion to the user. Enabling this feature for an application ensures that the remote AccessAgent is ready to do single sign-on when the user sees the logon prompt. 4. This feature is only applicable to a local AccessAgent automatically logging on to a remote AccessAgent. If there is no local AccessAgent or the local AccessAgent is not logged on, application launch is not delayed even if this feature is enabled. 5. This feature is not supported in AccessAdmin. To enable this feature, edit the values manually in the Windows registry.
Registry	`[DO] "TSDelayAppLaunchEnabled"`
Type	DWORD
Values	• #1: Yes • #0: No (default value)
Scope	Machine
Note	Refreshed on use.

pid_ts_delay_app_launch_timeout_secs: TSDelayAppLaunchTimeoutSecs

Location	**Registry Editor** > **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **IBM** > **ISAM ESSO** > **ECSS** > **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 single sign-on to be ready. If a remote AccessAgent is not ready for single sign-on in the timeout duration, the application launches. 5. The user might wait up to two times the timeout duration if the local AccessAgent manages to connect with a remote AccessAgent before the lapse of the first timeout duration. 6. This feature is not supported in AccessAdmin. To enable this feature, edit the values manually in the Windows registry.
Registry	`[DO] "TSDelayAppLaunchTimeoutSecs"`
Type	DWORD

pid_ts_delay_app_launch_timeout_secs: TSDelayAppLaunchTimeoutSecs

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: Actions on remote session while locking the local computer

IMS Entry	Actions on remote session while locking the local computer
Location	**AccessAdmin** > **User Policy Templates** > **New template** > **Create new policy template** > **AccessAgent Policies** > **Roaming Session Policies**
Description	Option to disconnect the Terminal Server or Citrix session, or log off from the remote AccessAgent while locking the local computer.
Registry	
Type	Non-negative integer
Values	• #0: No action (default value) • #1: Disconnect remote session • #2: Log off remote AccessAgent and disconnect remote session • #3: Log off remote session • #4: Log off remote AccessAgent
Scope	User
Note	Refreshed on sync.

pid_ts_logoff_local_session_action: Actions on remote session before logging off local session

IMS Entry	Actions on remote session before logging off local session
Location	**AccessAdmin** > **User Policy Templates** > **New template** > **Create new policy template** > **AccessAgent Policies** > **Roaming Session Policies**
Description	Option to disconnect the Terminal Server or Citrix session, or log off from the remote AccessAgent before logoff from the local AccessAgent.
Registry	
Type	Non-negative integer
Values	• #0: No action • #1: Disconnect remote session • #2: Log off remote AccessAgent and disconnect remote session (default value) • #3: Log off remote session • #4: Log off remote AccessAgent
Scope	User
Note	Refreshed on sync.

Log on/Log off policies

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

pid_script_logon_enabled: Enable logon script during user logon?

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	• #True: Yes • #False: No (default value)
Scope	User
Note	Refreshed on sync.

pid_script_logon_type: Logon script 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: Logon script 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: Enable logoff script during user logoff?

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	• #True: Yes • #False: No (default value)
Scope	User
Note	Refreshed on sync.

pid_script_logoff_type: Logoff script type

IMS Entry	Logoff script type
Location	**AccessAdmin** > **User Policy Templates** > **New template** > **Create new policy template** > **AccessAgent Policies** > **Logon/Logoff Policies**
Description	Type of logoff script to run. **Note:** Effective only if script logoff is enabled.
Registry	
Type	Positive integer
Values	• #1: Batch (default) • #2: VBScript
Scope	User
Note	Refreshed on sync.

pid_script_logoff_code: Logoff script 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: Allow user to manually log off AccessAgent

IMS Entry	Allow user to manually log off AccessAgent?

pid_logoff_manual_enabled: 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 the 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	• #1: Yes (default value) • #0: No • #True: Yes (default value) • #False: No
Scope	Machine User
Note	Refreshed on sync.

pid_logoff_manual_action: Actions on manual logoff by user

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 done 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	• #1: Log off Windows • #2: Log off Wallet (default value) • #4: Log off Wallet and lock computer

pid_logoff_manual_action: Actions on manual logoff by user

Scope	Machine User
Note	• Refreshed on sync for user policy. • Refreshed on use for machine policy.

pid_logoff_manual_action_countdown_secs: Confirmation countdown duration, in seconds, for manual logoff by user

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. Set the value to 0 to disable confirmation countdown. **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.
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: Enable Network Provider?

IMS Entry	Enable Network Provider?
Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **Logon/Logoff Policies**

pid_en_network_provider_enabled: Enable Network Provider?

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 Credential Provider. 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	• #1: Yes • #0: No (default value)
Scope	Machine
Note	Refreshed on use.

pid_logon_user_name_prefill_option: User name prefill option

IMS Entry	User name prefill option
Location	**AccessAdmin** > **Machine Policy Templates** > **New template** > **Create new machine policy template** > **AccessAgent Policies** > **Logon/Logoff Policies**
Description	Option for pre-filling the AccessAgent 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	• #0: Do not prefill. • #1: Prefill with last logged on user name. (default value) • #2: Prefill with currently logged on Windows user name.
Scope	Machine
Note	Refreshed on use.

pid_logon_user_name_display_option: 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**

pid_logon_user_name_display_option: User name display option

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 display about 20 characters only. If the name is truncated, it is appended with "...". 3. This policy affects the entire AccessAgent UI where the user name is displayed (for example, main UI, locked screen). 4. In a two-factor deployment (RFID, smart card, and others), the user does not need a user name to log on to AccessAgent. If the user forgets the second factor, the user must enter a user name and password to log on to AccessAgent or AccessAssistant. If the full name is always displayed, the user might forget the logon user name, because they do not use it every day and also do not see it in the AccessAgent user interface. As a best practice, policy value 1 must be used for a two-factor deployment.
Registry	`[DO] "LogonUserNameDisplayOption"`
Type	DWORD
Values	• 1 - User name (default value) • 2 - Given name followed by family name • 3 - Family name followed by given name
Scope	Machine
Note	Refreshed on logon.

pid_logoff_app_timeout_secs: Timeout, in seconds, for application logoff

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: Default action for applications, when user logs off

IMS Entry	Default action for applications, when user logs off AccessAgent
Location	**AccessAdmin** > **System** > **System policies** > **AccessAgent Policies** > **Logon/Logoff Policies**
Description	Default action to take for all applications when the user logs off AccessAgent. To log off applications, the AccessProfile for each application must contain a logoff action, otherwise the application is not logged off. **Note:** 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 is not logged off. 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	• #1: Log off the application • #2: Close the application • #3: Do nothing (default value)
Scope	System
Note	Refreshed on sync.

Hot Key policies

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

pid_enc_hot_key_enabled: Enable ISAM ESSO Hot Key?

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 ESSO Credential Provider, 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.

pid_enc_hot_key_enabled: Enable ISAM ESSO Hot Key?

Registry	`[DO] "EncHotKeyEnabled"`
Type	DWORD Boolean
Values	• #1: Yes (default value) • #0: No • #True: Yes (default value) • #False: No
Scope	Machine System
Note	Refreshed on startup.

pid_enc_hot_key_sequence: ISAM ESSO 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. Maximum of 3 keys from the set: {Ctrl, Shift, Alt, Ins, Del, Home, End, PgUp, PgDn, Break, E}. **Note:** 1. Effective only if `pid_enc_hot_key_enabled` is enabled. 2. Modifying this policy requires a computer restart to implement the changes.
Registry	`[DO] "EncHotKeySequence"`
Type	MULTI_SZ String list
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: ISAM ESSO Hot Key press actions at desktop when AccessAgent is logged on

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 done by AccessAgent if the ISAM ESSO 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	• #0: No action • #1: Log off Windows • #2: Log off Wallet • #4: Lock computer • #5: Log off Wallet and lock computer • #9: Launch AccessAgent window (default value)
Scope	Machine System
Note	• Refreshed on sync for system policy. • Refreshed on use for machine policy.

pid_enc_hot_key_action_countdown_secs: Confirmation countdown duration, in seconds, for pressing the ISAM ESSO Hot Key

IMS Entry	Confirmation countdown duration, in seconds, for pressing the 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**

pid_enc_hot_key_action_countdown_secs: Confirmation countdown duration, in seconds, for pressing the ISAM ESSO Hot Key

Description	Confirmation countdown duration, in seconds, for pressing the IBM Security Access Manager for Enterprise Single Sign-On Hot Key. Set the value to 0 to disable confirmation countdown. **Note:** 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: ISAM ESSO Hot Key press actions at desktop when AccessAgent is not logged on

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 done by AccessAgent if the IBM Security Access Manager for Enterprise Single Sign-On Hot Key is pressed at the desktop when a user is not logged on to AccessAgent. **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.
Registry	`[DO] "EncHotKeyNotLoggedOnAction"`
Type	DWORD Non-negative integer

pid_enc_hot_key_not_logged_on_action: ISAM ESSO Hot Key press actions at desktop when AccessAgent is not logged on

Values	• #0: No action • #1: Log off Windows • #4: Lock computer • #9: Launch AccessAgent window (default value)
Scope	Machine System
Note	• 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: Enable audit logging by AccessAgent

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	• #1: Yes (default value) • #0: No
Scope	Machine
Note	Refreshed on sync.

Background authentication policies

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

pid_background_auth_option: Option to perform background authentication

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

pid_background_auth_option: Option to perform background authentication

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: Time interval in minutes to initiate background authentication

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 re-attempt background authentication • >0: Interval in minutes
Scope	Machine
Note	

Network policies

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

pid_net_socket_timeout_secs: Timeout, in seconds, for making network socket connection

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: Timeout, in seconds, for making a SOAP call

IMS Entry	Timeout, in seconds, for making a SOAP call

pid_net_soap_timeout_secs: Timeout, in seconds, for making a SOAP call

Location	**AccessAdmin > Machine Policy Templates > New template > Create new machine policy > AccessAgent Policies > Network Policies**
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 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.

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: Require re-authentication before single sign-on?

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

© Copyright IBM Corp. 2002, 2015

pid_app_reauth_with_enc_pwd_enabled: Require re-authentication before single sign-on?

Values	• #True: Yes • #False: No (default value)
Scope	System
Note	Refreshed on sync.

pid_app_inject_pwd_entry_option_default: Default single sign-on password entry option for the application

IMS Entry	Default single sign-on password entry option for the application
Location	**AccessAdmin** > **System** > **Application policies** > **<*Application name*>** > **Application Policies**
Description	Default single sign-on password entry option for the application. **Note:** This policy overrides the system-wide and the authentication service default single sign-on password entry options.
Registry	
Type	Positive integer
Values	• #1: Automatic log on • #2: Always (default value) • #3: Ask • #4: Never • #5: Certificate
Scope	System
Note	Refreshed on sync.

pid_app_wallet_logoff_action: Action for the application, when user logs off AccessAgent

IMS Entry	Action for the application, when user logs off AccessAgent
Location	**AccessAdmin** > **System** > **Application policies** > **<*Application name*>** > **Application Policies**
Description	Default action for the application when the user logs off from AccessAgent. This policy overrides the corresponding system-wide policy. The AccessProfile for the application must contain a logoff action, otherwise the application is not logged off. **Note:** 1. This policy overrides Wallet logoff action for applications default. 2. See the notes for Wallet logoff action for applications default. 3. For web applications, each URL is considered an application. Microsoft Internet Explorer is also considered an application. In this context, the web application policy overrides the Microsoft Internet Explorer policy, which overrides Wallet logoff action for applications default. 4. For Microsoft Internet Explorer and Windows Explorer, you can set the value to either 2 or 3. 5. This policy is set to 3 for Windows logon (application Credential Provider) when the IMS Server is installed.

pid_app_wallet_logoff_action: Action for the application, when user logs off AccessAgent

Registry	
Type	Positive integer
Values	• #1: Log off the application • #2: Close the application • #3: Do nothing (default value)
Scope	System
Note	Refreshed on use.

Authentication service policies

View the details of the different authentication service policies.

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: Enable manual password change with random password?

IMS Entry	Enable manual password change with random password?
Location	**AccessAdmin** > **User Policy Templates** > **New template** > **Create new policy template** > **Authentication Service Policies** > ***<Authentication service name>***
Description	Whether manual password change with a random password is enabled for the authentication service.
Registry	
Type	Boolean
Values	• #True: Yes • #False: No (default value)
Scope	User
Note	Refreshed on sync.

pid_auth_reauth_with_enc_pwd_enabled: Require re-authentication before single sign-on?

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

pid_auth_reauth_with_enc_pwd_enabled: Require re-authentication before single sign-on?

Values	• #True: Yes • #False: No (default value)
Scope	System
Note	Refreshed on sync.

pid_auth_pwd_is_ad_pwd: Is the password the Windows logon password?

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	• #True: Yes • #False: No (default value)
Scope	System
Note	Refreshed on use.

pid_enc_pwd_min_length: Minimum password 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: Maximum password length

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

pid_enc_pwd_max_length: Maximum password length

Scope	System
Note	• The value can range from 1 to 99. • Refreshed on sync.

pid_enc_pwd_min_numerics_length: Minimum number of numeric characters

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: Minimum number of alphabetic characters

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: Minimum number of special characters

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)

pid_auth_fortification_pwd_min_special_characters_length: Minimum number of special characters

Scope	System
Note	• The value can range from `0` to `99`. • Refreshed on sync.

pid_auth_fortification_pwd_max_numerics_length: Maximum number of numeric characters

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: Maximum number of alphabetic characters

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: Maximum number of special characters

IMS Entry	Maximum number of special characters
Location	**AccessAdmin** > **System** > **Authentication service policies** > **<*Authentication service name*>** > **Password Policies**

pid_auth_fortification_max_special_characters_length: Maximum number of special characters

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
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: Enforce the use of both upper case and lower case characters?

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	• #True: Yes • #False: No (default value)
Scope	System
Note	Refreshed on sync.

Authentication policies

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

pid_auth_is_enterprise: Is it an enterprise authentication service?

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	• #True: Yes • #False: No (default value)
Scope	System

pid_auth_is_enterprise: Is it an enterprise authentication service?

Note	Refreshed on sync.

pid_auth_inject_pwd_entry_option_default: Default single sign-on password entry option for the authentication service

IMS Entry	Default single sign-on password entry option for the authentication service
Location	**AccessAdmin** > **System** > **Authentication service policies** > **<*Authentication service name*>** > **Authentication Policies**
Description	Default single sign-on password entry option for the authentication service. **Note:** 1. Effective only if `pid_auth_is_enterprise` is enabled for the authentication service. 2. Overrides Wallet inject password entry option default.
Registry	
Type	Positive integer
Values	• #1: Automatic log on • #2: Always (default value) • #3: Ask • #4: Never • #5: Certificate
Scope	System
Note	Refreshed on sync.

pid_auth_authentication_option: Authentication modes to be supported

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	• #1: Password (default value) • #2: SCR • #4: CAPI • #32 : CCOW
Scope	System
Note	• You can select multiple values. • Refreshed on sync.

pid_auth_capture_prompt_enabled: Prompt user on auto-capture of password?

IMS Entry	Prompt user on auto-capture of password?
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	• #True: Yes (default value) • #False: No
Scope	System
Note	Refreshed on sync.

pid_auth_accounts_max: Maximum number of accounts allowed for the authentication service

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 reach or exceed the maximum that is 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 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

pid_auth_accounts_max: Maximum number of accounts allowed for the authentication service

Note	• The value can range from `0` to `10`. • Refreshed on sync.

Chapter 13. Policies for Privileged Identity Management

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

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

IBM Security Privileged Identity Manager configuration policies

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

pid_pim_cico_svc_url: IBM Security Privileged Identity Manager URL

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

pid_pim_itim_auth_svc_id: IBM Security Privileged Identity Manager Authentication Service ID

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

pid_recorder_enabled: Enable session recording?

IMS Entry	Enable session recording?

© Copyright IBM Corp. 2002, 2015

pid_recorder_enabled: Enable session recording?

Location	**AccessAdmin > System > System policies > IBM Security Privileged Identity Manager Configuration Policies**
Description	Whether to record sessions created using shared access identities.
Registry	
Type	Boolean
Values	• No • Yes (default, if session recording feature is activated)
Scope	System
Note	Refreshed on sync.

pid_recorder_server: Privileged Session Recorder Server URL

IMS Entry	Privileged Session Recorder Server URL
Location	**AccessAdmin > System > System policies > IBM Security Privileged Identity Manager Configuration Policies**
Description	URL of the Privileged Session Recorder Server. For example: `https://psr.example.com/recorder/collector`
Registry	
Type	
Values	String
Scope	System
Note	Refreshed on sync.

pid_recorder_image_capture_option: Session recording image capture option

IMS Entry	Session recording image capture option
Location	**AccessAdmin > System > System policies > IBM Security Privileged Identity Manager Configuration Policies**
Description	Color depth of the images to capture for session recording.
Registry	
Type	Non-negative integer
Values	• #0: Full Color • #1: Grayscale (default value)
Scope	System
Note	Refreshed on sync.

pid_recorder_keyboard_capture_option: Session recording keyboard capture option

IMS Entry	Session recording keyboard capture option
Location	**AccessAdmin > System > System policies > IBM Security Privileged Identity Manager Configuration Policies**

pid_recorder_keyboard_capture_option: Session recording keyboard capture option

Description	Specifies keyboard events to capture during a screen-based session recording.
Registry	
Type	Non-negative integer
Values	• #0: Log all key inputs (default value) • #1: Log only special keys • #2: Do not log any key inputs
Scope	System
Note	Refreshed on sync. This option does not apply to text-based recordings.

pid_collector_comm_fail_action: Action to take when the client computer cannot connect to the server

IMS Entry	Action to take when the client computer cannot connect to the server
Location	**AccessAdmin** > **System** > **System policies** > **IBM Security Privileged Identity Manager Configuration Policies**
Description	Specifies the action to take on the client computer when the Privileged Session Recorder Server is not reachable after a maximum number of retries.
Registry	
Type	Non-negative integer
Values	• #0: Take no action. • #1: Block user inputs. • #2: Close application.
Scope	System
Note	Refreshed on sync.

pid_collector_comm_fail_limit: Maximum number of failed connection attempts to the server

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

pid_collector_comm_fail_retry_interval: Time interval between connection retries to the Privileged Session Recorder Server

IMS Entry	Time interval between connection retries to the Privileged Session Recorder Server
Location	**AccessAdmin > System > System policies > IBM Security Privileged Identity Manager Configuration Policies**
Description	Time interval, in seconds, between attempts to connect to the Privileged Session Recorder Server.
Registry	
Type	Non-negative integer
Values	15 (default value)
Scope	System
Note	Refreshed on sync.

pid_pim_optional_justification: Allow empty justification on credential check-out

IMS Entry	Allow empty justification on credential check-out
Location	**AccessAdmin > System > System policies > IBM Security Privileged Identity Manager Configuration Policies**
Description	Specifies whether users can check out credentials from AccessAgent without providing any justification.
Registry	
Type	Boolean
Values	• #False: No (default value) • #True: Yes
Scope	System
Note	Refreshed on sync.

Chapter 14. Other policies

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

AAOnlineHelpLink

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	http://www.ibm.com/support/knowledgecenter/SS9JLE_8.2.2 (default value)
Scope	
Note	Set this policy to empty to remove the Help link from the AccessAgent user interface. To specify another URL for the Help link, you can replace the default value with another URL.

ObsOnlineHelpEnabled

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	

WindowsEventLogEnabled

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	

SystemModalMessageEnabled

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

© Copyright IBM Corp. 2002, 2015

SystemModalMessageEnabled

Registry	`[DO] "SystemModalMessageEnabled"`
Type	DWORD
Values	• #0: Disables the System Modal message box (default value) • #1: Enables the System Modal message box
Scope	
Note	

UIDirectionLToR

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	

Chapter 15. Policy limitations in Windows 7 and above

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 7
No action	Works as expected
Lock computer	Works as expected
Log off Wallet and lock computer	Works as expected
Switch user	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	Does not work

- **pid_fingerprint_tap_different_action**

Option	Action in Windows 7
No action	Works as expected
Lock computer	Works as expected
Log off Wallet and lock computer	Works as expected
Switch user	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	Does not work

© Copyright IBM Corp. 2002, 2015

Notices

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

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

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

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

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

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

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

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

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

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

© Copyright IBM Corp. 2002, 2015

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

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

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

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

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

Trademarks

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

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

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

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

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

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

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

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

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

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

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

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

Privacy Policy Considerations

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

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

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

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

Glossary

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

The following cross-references are used in this glossary:

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

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

A

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

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

account data item
The user credentials required for logon.

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

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

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

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential
The Active Directory user name and password.

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

active radio frequency identification (active RFID) A second authentication factor and presence detector. See also radio frequency identification.

active RFID
See active radio frequency identification.

AD See Active Directory.

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

API See application programming interface.

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

application policy
A collection of policies and attributes governing access to applications.

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

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

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

© Copyright IBM Corp. 2002, 2015

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

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

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

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

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

B

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

base image
A template for a virtual desktop.

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

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

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

C

CA See certificate authority.

CAPI See cryptographic application programming interface.

Card Serial Number (CSN)
A unique data item that identifies a hybrid smart card. It has no relation to the certificates installed in the smart card

CCOW
See Clinical Context Object Workgroup.

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

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

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

CLI See command-line interface.

Clinical Context Object Workgroup (CCOW)
A vendor independent standard, for the interchange of information between clinical applications in the healthcare industry.

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

command-line interface (CLI)
A computer interface in which the input and output are text based.

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

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

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

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

CSN See Card Serial Number.

CSP See cryptographic service provider.

D

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

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

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

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

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

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

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

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

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

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

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

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

DLL See dynamic link library.

DN See distinguished name.

DNS See domain name server.

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

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

E

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

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

ESSO See enterprise single sign-on.

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

F

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

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

Federal Information Processing Standard (FIPS)
A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

FIPS See Federal Information Processing Standard.

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

FQDN
See fully qualified domain name.

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

G

GINA See graphical identification and authentication.

GPO See group policy object.

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

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

H

HA See high availability.

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

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

hot key
A key sequence used to shift operations

between different applications or between different functions of an application.

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

I

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

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

J

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

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

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

JMX See Java Management Extensions.

JRE See Java runtime environment.

JVM See Java virtual machine.

K

keystore
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

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

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

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

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

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

M

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

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

N

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

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

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

O

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

OTP See one-time password.

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

P

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

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

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

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

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

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

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

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

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

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

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

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

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

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

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

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

R

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

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

RDP See remote desktop protocol.

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

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

remote desktop protocol (RDP)
A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

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

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

RFID See radio frequency identification.

root CA
See root certificate authority.

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

S

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

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

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

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

Secure Sockets Layer virtual private network (SSL VPN)
A form of VPN that can be used with a standard web browser.

Security Token Service (STS)
A web service that is used for issuing and exchanging security tokens.

security trust service chain
A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

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

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

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

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

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

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

sign up
To request a resource.

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

Simple Mail Transfer Protocol (SMTP)
An Internet application protocol for transferring mail among users of the Internet.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

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

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

SMTP See Simple Mail Transfer Protocol.

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

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

SPI See service provider interface.

SSL See Secure Sockets Layer.

SSL VPN
See Secure Sockets Layer virtual private network.

SSO See single sign-on.

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

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

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

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

STS See Security Token Service.

system modal message
A system dialog box that is typically used to display important messages. When a system modal message is displayed,

nothing else can be selected on the screen until the message is closed.

T

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

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

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

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

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

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

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

tty See terminal type.

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

U

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

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

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

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

V

VB See Visual Basic.

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

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

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

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

Virtual Member Manager (VMM)
A WebSphere Application Server component that provides applications with a secure facility to access basic

organizational entity data such as people, logon accounts, and security roles.

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

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

VMM See Virtual Member Manager.

VPN See virtual private network.

W

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

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

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

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

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

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

Index

A

AccessAgent policies 45
  behavior 53, 107
  user interface 53
accessibility v
accessibility policies 36
audit logging policies 41, 104
audit settings 41
authentication factor policies 7
authentication policies 7
authentication services policies 107, 109, 113

B

background authentication policies 104
bidirectional support policy 121

C

change password 9
Citrix Server policies 39
customize text 21

D

desktop inactivity policies 59
display policies 53

E

education v
ESSO Credential Provider policies
  behavior 55
  configurable text 21

F

fingerprint authentication policies 83

G

glossary 129

H

hot key policies 100
hybrid smart card authentication policies 72

I

IBM
  Software Support v
  Support Assistant v

L

lightweight mode policies 39
lock/unlock policies 63
log file policies 43
log on/log off policies 94
log policies 41

N

network policies 41, 105

O

online help policy 121

P

password aging policies 9
password change policies 11
password policies 109
password strength policies 9, 12
policies 117
  about 1
  accessibility 36
  application 107
  audit logging 104
  authentication 7, 113
  authentication service 109
  background authentication 104
  desktop inactivity 59
  ESSO Credential Provider 55
  fingerprint 83
  hot key 100
  hybrid smart card 72
  legends 3
  lightweight mode 39
  lock/unlock 63
  log on/log off 94
  logs 43
  network 105
  password 109
  password aging 9
  password change 11
  password strength 12
  registry 121
  RFID 76
  roaming session 93
  self-service password reset 15
  self-service registration 16
  set priorities 5
  shared desktop 37
  sign up 17
  smart card 71
  symbols 3
  temporary file 43
  Terminal Server 87
  troubleshooting 41
  view priorities 5
  Wallet 45
policies *(continued)*
  window display 53
policy limitations 123
private desktop policies 37
Privileged Identity Management policies 117
problem-determination v
publications
  statement of good security practices v

R

registry policies 121
RFID policies 76
roaming session policies 93

S

second factor bypass 16
self-service password reset policies 15
self-service registration policies 16
session recording policies 117
shared desktop policies 37
sign up policies 15
  configurable text 35
  customize 17
smart card authentication policies 71
system modal message policy 121

T

temporary file policies 41, 43
Terminal Server policies 39, 87
text policies
  ESSO Credential Provider 21
  ESSO GINA 21
  sign up 35
  unlock 25
  user interface 21
training v
troubleshooting policies 41

U

unlock text policies 25
user interface 21, 53

W

Wallet policies 45
Windows 7 limitations 123
windows event log policy 121

© Copyright IBM Corp. 2002, 2015

Printed in USA