Product Documentation

PAM

System Properties Reference Guide

Contents

System Properties Reference Guide

Download (docx)

Backend Database

Property	Default	Description
derby.system.home		Embedded database home folder
hibernate.connection.driver_class		Backend database driver class
hibernate.dialect		Backend database dialect
pam.db.password		Backend database Password
pam.db.url		Backend database URL
pam.db.user		Backend database User
pam.db.validationQuery		Test backend database query to validate connection

LDAP Authentication

Property	Default	Description
ldap.authn.searchFilter		Main integrated LDAP user search filter
ldap.baseDn		Main integrated LDAP base DN
ldap.domain		Main integrated LDAP domain
ldap.groupSearch		Main integrated LDAP groups search query
ldap.managerDn		Main integrated LDAP service account
ldap.managerPassword		Main integrated LDAP service account password
ldap.roleBase		Main integrated LDAP base tree node for groups
ldap.roleName	cn	Main integrated LDAP attribute name for a group name
ldap.roleSearch		Main integrated LDAP role search query

Property	Default	Description
ldap.rootDn		Main integrated LDAP root DN
ldap.url		Main integrated LDAP URL
realm.apacheds.local.baseDn		Local user directory service account DN
realm.apacheds.local.bindCredentials		Local user directory service account password
realm.apacheds.local.connectionURL		Local user directory URL
realm.apacheds.local.groupSearch		Local user directory group search query
realm.apacheds.local.roleBase		Local user directory group base
realm.apacheds.local.roleName		Local user directory attribute for group name
realm.apacheds.local.roleSearch		Local user directory membership search query
realm.apacheds.local.userBase		Local user directory user base
realm.apacheds.local.userSearch		Local user directory user search query
realm.apacheds.local.userSearch.cas		Local user directory user search for CAS
ldap[2].name		Integration name
ldap[2].url		LDAP URL
ldap[2].managerDn		Service account DN
ldap[2].managerPassword		Service account DN password
ldap[2].rootDn		Root DN
ldap[2].baseDn		Base DN
ldap[2].domain		Domain
ldap[2].authn.searchFilter		User search filter
ldap[2].userName	uid	User name attribute
ldap[2].userSearch		User search filter
ldap[2].roleBase		Role base DN
ldap[2].roleName	cn	Role name attribute
ldap[2].roleSearch		Search query for roles by user
ldap[2].groupSearch		Search query for roles

MFA

Property	Default	Description
cas.authn.mfa.duo[0].duoApiHost		Duo MFA integration Duo Security API URL
cas.authn.mfa.duo[0].duoApplicationKey		Duo MFA integration application or secret key
cas.authn.mfa.duo[0].duoIntegrationKey		Duo MFA integration API key
cas.authn.mfa.duo[0].duoSecretKey		Duo MFA integration secret key
cas.authn.mfa.duo[0].id		Duo MFA integration ID (mfa-duo)
cas.authn.mfa.duo[0].name		Duo MFA integration name
cas.authn.mfa.duo[0].rank	0	Duo MFA integration rank
cas.authn.mfa.duo[0].trustedDeviceEnabled	False	Duo MFA integration flag to enable trusted devices option
cas.authn.mfa.gauth.codeDigits	6	TOTP MFA number of digits in the code
cas.authn.mfa.gauth.issuer		TOTP MFA issuer
cas.authn.mfa.gauth.jpa.database.dataSourceName		TOTP MFA database connection (usually java:comp/env/jdbc/PamDB)
cas.authn.mfa.gauth.jpa.database.dataSourceProxy	true	TOTP MFA data source proxy
cas.authn.mfa.gauth.jpa.database.ddlAuto	update	TOTP MFA database pre-creation option
cas.authn.mfa.gauth.jpa.database.dialect		TOTP MFA database dialect (usually {hibernate.dialect})
cas.authn.mfa.gauth.jpa.database.driverClass		TOTP MFA database driver class (usually {hibernate.connection.driver_class})
cas.authn.mfa.gauth.label		TOTP MFA screen label
cas.authn.mfa.gauth.timeStepSize	30	TOTP MFA time step size

Property	Default	Description
cas.authn.mfa.gauth.trustedDeviceEnabled	False	TOTP MFA flag to enable trusted devices option
cas.authn.mfa.gauth.windowSize	3	TOTP MFA window size
cas.authn.mfa.globalProviderId		Global MFA provider
cas.authn.mfa.radius.client.accountingPort		Radius MFA accounting port
cas.authn.mfa.radius.client.authenticationPort		Radius MFA authentication port
cas.authn.mfa.radius.client.inetAddress		Radius MFA host name or IP address
cas.authn.mfa.radius.client.sharedSecret		Radius MFA secret
cas.authn.mfa.radius.server.protocol		Radius MFA server protocol
cas.authn.mfa.yubikey.clientId		Yubikey MFA client ID
cas.authn.mfa.yubikey.jpa.dataSourceName		Yubikey MFA data source name (usually java:comp/env/jdbc/PamDB)
cas.authn.mfa.yubikey.jpa.dataSourceProxy	true	Yubikey MFA data source proxy
cas.authn.mfa.yubikey.jpa.ddlAuto	update	Yubikey MFA database pre-creation option
cas.authn.mfa.yubikey.jpa.dialect		Yubikey MFA database dialect (usually {hibernate.dialect})
cas.authn.mfa.yubikey.jpa.driverClass		Yubikey MFA database driver class (usually {hibernate.connection.driver_class})
cas.authn.mfa.yubikey.name		Yubikey MFA integration name
cas.authn.mfa.yubikey.secretKey		Yubikey MFA secret key
cas.authn.mfa.groovyScript		Path to Groovy script to enable granular MFA integration

CAS

Property	Default	Description
cas.audit.alternateClientAddrHeaderName		HTTP Header for client address (X-Forwarded-For)
cas.audit.jdbc.dataSourceName		CAS audit data source name (usually java:comp/env/jdbc/PamDB)
cas.audit.jdbc.dataSourceProxy		CAS audit MFA data source proxy
cas.audit.jdbc.ddlAuto	update	CAS audit database pre-creation option
cas.audit.jdbc.dialect		CAS audit database dialect (usually {hibernate.dialect})
cas.audit.jdbc.driverClass		CAS audit database driver class (usually {hibernate.connection.driver_class})
cas.authn.accept.users	Empty	Hard coded users for authentication
cas.clearpass.cacheCredential	False	Flag to enable using the password of the current user for system operations such as session connect
cas.clearpass.cacheCredential	true	Flag to enable pass-through credentials capture
cas.clearpass.crypto.enabled	true	Flag to enable pass-through credential encryption
cas.clearpass.crypto.encryption.key		Pass-through credentials encryption key
cas.clearpass.crypto.signing.key		Pass-through credentials sining key
cas.logout.confirmLogout	true	Confirms CAS logout
cas.logout.followServiceRedirects	true	Flag to enable service provider logout for SAML integrated providers
cas.managed.path		Application Access URL stem (https://xtam.company.com/
cas.metrics.loggerName		
cas.metrics.refreshInterval	86400	

Property	Default	Description
cas.server.name		Managed path of CAS server URL (for example, https://xtam.company.com)
cas.server.prefix		CAS URL for SAML integration (for example, https://xtam.company.com/xtam/)
cas.serviceRegistry.initFromJson	true	Flag for CAS registry DB initialization
cas.serviceRegistry.jpa.dataSourceName		CAS service registry data source name (usually java:comp/env/jdbc/PamDB)
cas.serviceRegistry.jpa.dataSourceProxy	true	CAS service registry MFA data source proxy
cas.serviceRegistry.jpa.ddlAuto	update	CAS service registry database pre-creation option
cas.serviceRegistry.jpa.dialect		CAS service registry database dialect (usually {hibernate.dialect})
cas.serviceRegistry.jpa.driverClass		CAS service registry database driver class (usually {hibernate.connection.driver_class})
cas.standalone.config.security.alg		Algorithm for CAS parameters encryption
cas.standalone.config.security.psw		Master password to encrypt CAS parameters
cas.tgc.crypto.enabled	true	Flag to enable CAS TGC encryption
cas.tgc.crypto.encryption.key	generated	CAS TGC encryption key
cas.tgc.crypto.signing.key		CAS ticket granting signing key. SRF token signing key
cas.tgc.crypto.signing.key	generated	CAS TGC signing key
cas.ticket.registry.cleaner.schedule.enabled		CAS ticket registry cleaner schedule enable flag
cas.ticket.registry.cleaner.schedule.repeatInterval		CAS ticket registry cleaner repeat interval
cas.ticket.registry.cleaner.schedule.startDelay		CAS ticket registry cleaner start delay
cas.ticket.registry.jpa.crypto.alg	AES	CAS ticket registry encryption algorithm
cas.ticket.registry.jpa.crypto.enabled	true	Flag to enable CAS registry encryption
cas.ticket.registry.jpa.crypto.encryption.key	generated	CAS ticket registry encryption key

Property	Default	Description
cas.ticket.registry.jpa.crypto.encryption.keySize	16	CAS ticket registry encryption key size
cas.ticket.registry.jpa.crypto.signing.key	generated	CAS ticket registry signing key
cas.ticket.registry.jpa.crypto.signing.keySize	512	CAS ticket registry signing key size
cas.ticket.registry.jpa.dataSourceName		CAS ticket registry data source name (usually java:comp/env/jdbc/PamDB)
cas.ticket.registry.jpa.dataSourceProxy	true	CAS ticket registry MFA data source proxy
cas.ticket.registry.jpa.ddlAuto	update	CAS ticket registry MFA database pre-creation option
cas.ticket.registry.jpa.dialect		CAS ticket registry database dialect (usually {hibernate.dialect})
cas.ticket.registry.jpa.driverClass		CAS ticket registry database driver class (usually {hibernate.connection.driver_class})
cas.ticket.registry.jpa.jpaLockingTimeout	3600	CAS ticket locking timeout
cas.ticket.registry.jpa.ticketLockType	NONE	CAS ticket lock shared among nodes
cas.ticket.st.timeToKillInSeconds	10	
cas.view.defaultRedirectUrl		Application Access URL such as https://xtam.company.com/xtam/
cas.webflow.crypto.alg	AES	
cas.webflow.crypto.enabled	true	
cas.webflow.crypto.encryption.key		CAS webflow encryption key
cas.webflow.crypto.encryption.keySize	16	
cas.webflow.crypto.signing.key		CAS webflow signing key
cas.webflow.crypto.signing.keySize	512	

CAS Authentication

Property	Default	Description
cas.authn.ldap[0].type	DIRECT	Local user directory type
cas.authn.ldap[0].ldapUrl		Local user directory URL
cas.authn.ldap[0].useSsl		Local user directory SSL enabling
cas.authn.ldap[0].useStartTls		Local user directory StartTLS enabling
cas.authn.ldap[0].connectTimeout		Local user directory connect timeout
cas.authn.ldap[0].baseDn		Local user directory base DN
cas.authn.ldap[0].userFilter		Local user directory filter to search users
cas.authn.ldap[0].subtreeSearch		Local user directory enable subtree search
cas.authn.ldap[0].usePasswordPolicy	false	Local user directory use password policy
cas.authn.ldap[0].dnFormat		Local user directory DN format pattern based on user entry
cas.authn.ldap[0].principalAttributeId	uid	Local user directory attribute for user
cas.authn.ldap[0].principalAttributeList		Local user directory list of attributes to retrieve from the directory
cas.authn.ldap[1].type		Integrated LDAP user directory type (AUTHENTICATED|AD|DIRECT|ANONYMOUS)
cas.authn.ldap[1].ldapUrl		Integrated LDAP user directory URL
cas.authn.ldap[1].useSsl		Integrated LDAP user directory use SSL option
cas.authn.ldap[1].useStartTls		Integrated LDAP user directory use StartTLS option
cas.authn.ldap[1].connectTimeout		Integrated LDAP user directory connection timeout
cas.authn.ldap[1].baseDn		Integrated LDAP user directory base DN
cas.authn.ldap[1].userFilter		Integrated LDAP user directory user query
cas.authn.ldap[1].subtreeSearch		Integrated LDAP user directory enable subtree search

Property	Default	Description
cas.authn.ldap[1].usePasswordPolicy	false	Integrated LDAP user directory password policy use
cas.authn.ldap[1].dnFormat		Integrated LDAP user directory DN format pattern
cas.authn.ldap[1].principalAttributeId		Integrated LDAP user directory attribute for user name (for example, sAMAccountName or UserPrincipalName)
cas.authn.ldap[1].principalAttributeList		Integrated LDAP user directory list of attributes to retrieve from directory
cas.authn.pac4j.saml[x].clientName		SAML integration client name
cas.authn.pac4j.saml[x].keystorePassword		SAML integration keystore password
cas.authn.pac4j.saml [x].privateKeyPassword		SAML integration
cas.authn.pac4j.saml [x].serviceProviderEntityId		SAML integration service provider entity ID
cas.authn.pac4j.saml [x].serviceProviderMetadataPath		SAML integration URL to service provider metadata
cas.authn.pac4j.saml[x].keystorePath		SAML integration path to keystore
cas.authn.pac4j.saml [x].identityProviderMetadataPath		SAML integration path to provider metadata file
cas.authn.pac4j.saml [x].maximumAuthenticationLifetime		SAML integration maximum authentication lifetime
cas.authn.pac4j.saml[x].forceAuth	false	SAML integration

XTAM

Property	Default	Description
ide	False	Flag to avoid 1-minute delay starting up worker processes
java.io.tmpdir		OS temporary folder

Property	Default	Description
java.net.useSystemProxies	true	Flag to disable use of OS proxy configuration for HTTP queries such as check for latest version. False in OOB configuration.
mail.smtp.timeout	10000	Timeout in milliseconds for SMTP operations
pam.language	en_US	Default language to initialize the system
user.home		Temporary folder base for the playback rendering
xtam.ad.members.search	true	Flag to enable dynamic reference from local groups to external LDAP members to allow entry reorganization in the external user directory without breaking local groups membership. When set to False, the system will use entry DN to reference external entry instead of search
xtam.api.token.verification	true	Flag to disable XSRF token verification
xtam.aws.sts.endpoint		AWS STS Endpoint for temporary ticket generation. The value defaults to sts.amazonaws.com and could be overwritten by record field STSEndpoint.
xtam.aws.sts.region		AWS STS Region for temporary ticket generation. The value defaults to us-east-1 and could be overwritten by record field STSRegion.
xtam.cas.mfa.token		Authentication token from CAS login process to XTAM granular MFA service
xtam.cas.mfa.default	none	Default MFA service to use in case of failure to detect user or group based MFA service
xtam.cas.registry.sqlCasJwtSigningKey		SQL statement for CAS registry
xtam.cas.registry.sqlCasJwtupdateService		SQL Statement for CAS registry update
xtam.cert.password		WEB Server SSL Certificate password
xtam.cert.path		Path to WEB Server SSL Certificate
xtam.config.recording.encrypt	False	Flag to enable encryption of session recordings
xtam.driver.wsman.delay	1	WS-Management protocol delay in seconds between commands

Property	Default	Description
xtam.driver.wsman.timeout	30	WS-Management protocol timeout in seconds
xtam.ha[0].url		Second node URL for node replication
xtam.http.proxy	False	Flag to enable HTTP Proxy in remote node to tunnel RDP, SSH and HTTP proxy connections from master node as a session manager
xtam.http.proxy.port		Port number overwrite for remote node HTTP Proxy serving as a session manager for master node proxy servers
xtam.http.proxy.upstream.auth.alg	SHA256	Encryption algorithm for remote Proxy session manager communication for SSH, RDP, HTTPs proxies
xtam.import.unique	False	Flag to enable enforcement of unique record names in folder during import process
xtam.integration.duo.apiHost		Overwrite for cas.authn.mfa.duo[0].duoApiHost
xtam.integration.duo.integrationKey		Overwrite for cas.authn.mfa.duo [0].duoIntegrationKey
xtam.integration.duo.secretKey		Overwrite for cas.authn.mfa.duo[0].duoSecretKey
xtam.integration.sms.password		
xtam.integration.sms.script		SMS integration Groovy script from script library
xtam.integration.sms.url		SMS integration URL
xtam.integration.sms.user		
xtam.integration.ticketing.password		Service account password for ticketing system integration
xtam.integration.ticketing.pattern		Request reason pattern indicating a message to ticketing system (SN #)
xtam.integration.ticketing.script		Groovy script from the script library to integration with ticketing system
xtam.integration.ticketing.url		URL of ticketing system
xtam.integration.ticketing.user		Service account for ticketing system integration

Property	Default	Description
xtam.item.name.length	3996	Max length of form fields
xtam.item.ref.credential.only	False	Flag to use only credential fields for reference records
xtam.mfa.mock	False	Flag enabling mock MFA controller (allow first time use, deny second time use)
xtam.perflog.dump_attributes	False	Flag to log operating system attributes to performance logging
xtam.perflog.enabled	False	Flag to enable internal performance logging
xtam.perflog.logging.file	Perf.log	File name for the internal performance logging if not redirected to system log
xtam.perflog.logging.level	INFO	Level of the system log message for internal performance log
xtam.perflog.logging.system	False	Flag to redirect internal performance logging to regular system logging instead of custom file perf.log
xtam.perflog.period.seconds	60	Period of internal performance logging
xtam.proxy.cli.mfa.disabled	False	Flag to disable capability to pass MFA token with RDP, SSH proxy user attribute
xtam.proxy.host		XTAM Proxy host if different from cas.managed.path (for example, for geo-distributed systems)
xtam.proxy.http.trustAllServers	False	Flag to enable HTTP Proxy to trust SSL Certificates of all endpoint WEB Portals
xtam.rdp.proxy	False	Flag to enforce RDP proxy startup
xtam.rdp.proxy.port		RDP Proxy port overwrite
xtam.rdp.proxy.trace_cleartext_credentials	False	Flag to enable tracing of credential capturing by the system
xtam.remote.enabled	False	Flag to switch the node to remote node mode
xtam.remote.node		Node name to overwrite default host name as a node name
xtam.remote.password		Remote node user password

Property	Default	Description
xtam.remote.token		Remote node authentication token as an alternative to user and password
xtam.remote.url		Master node URL
xtam.remote.user		Master node user to connect to master node
xtam.remote[0].enabled	false	Flag to enable master node configuration for multi-master node deployment
xtam.remote[0].url		Master node URL in multi-master node deployment
xtam.remote[0].user		Master node user in multi-master node deployment
xtam.remote[0].password		Master node password in multi-master node deployment
xtam.remote[0].token		Master node password token in multi-master node deployment to use instead of user and password
xtam.replication.signingKey		Signing key for node-to-node replication exchange
xtam.report.daily.hours	0	Hour for the daily report schedule
xtam.report.monthly.days	1	Day of the month for monthly report schedule
xtam.report.weekly.days	SUN	Day of the week for weekly report schedule
xtam.secured.ids	False	Flag to enable Secure-IDs
xtam.secured.ids.strict	False	Flag to enable strict check for Secure-IDs
xtam.session.command.input.wait	1000	Time in milliseconds to wait before issuing blocking command (such as sudo) at the start of remote session
xtam.shadow.crossvault.disable	False	Flag to disable restriction to make reference, shadow and dynamic credential records in another vault
xtam.proxy.mfa.disable	False	Flag to disable MFA for proxy sessions (SSH, RDP, HTTP). This parameter replaced now deprecated but still valid parameter xtam.ssh.proxy.mfa.disable with the same meaning.
xtam.ssh.session.idle	0	Default idle timeout for SSH sessions

Property	Default	Description
xtam.transport.security.bc	false	Flag to enable Bouncy Castle installed as a preferred security provider
xtam.ueba.enabled	true	Flag to enable business analytics processing
xtam.user.guest.enabled	false	Flag to enable auto-creating guest accounts authenticated using external SSO services
xtam.user.guest.group		Local group to add auto-created guest user
xtam.user.guest.ttl	0	Expiration time in milliseconds (0 – infinite) for auto-created guest user
xtam.web.mfa.disable	false	Flag to disable MFA for WEB Login (as oppose to Proxy Servers)
xtam.ssh.proxy.connect_retry_count	2	Number of times SSH Proxy will retry connecting to remote server
xtam.ssh.proxy.auth_retry_count	5	Number of times SSH Proxy will retry authenticating XTAM user
xtam.ssh.proxy.connect_retry_timeout	10	Number of seconds SSH Proxy waits before retrying to connect to remote server progressively increasing with each retry (10 seconds after first failed attempt, 20 seconds after seconds one, 30 seconds after third one)
xtam.ssh.proxy.auth_retry_timeout	10	Number of seconds SSH Proxy waits before retrying to authenticate XTAM user progressively increasing with each retry (10 seconds after first failed attempt, 20 seconds after seconds one, 30 seconds after third one)
xtam.ssh.exec.su.mode	1	SSH su command execution mode: 1 - su - user -c 'command' 2 - su -c 'command' - user
xtam.ssh.exec.verify.feedback	false	Default SSH execution strategy password reset verification only checks successful connectivity with new password. Set this option to true to verify password reset by checking the output from the echo command to confirm successful command execution.

Property	Default	Description
xtam.ssh.channel.connect.timeout	20000	Timeout opening SSH job execution channel in milliseconds. Default is defined by the library and is about 20 seconds (20000 ms)
xtam.session.command.expect.su	password	Expected output for su command to type password
xtam.reverse.tunnel[0].remoteHost		Master node host for SSH connection for reverse tunnel configuration
xtam.reverse.tunnel[0].remotePort		Master node port for SSH connection for reverse tunnel configuration
xtam.reverse.tunnel[0].remoteUser		Master node user for SSH connection for reverse tunnel configuration
xtam.reverse.tunnel[0].remotePassword		Master node user password or Private Key password for SSH connection for reverse tunnel configuration
xtam.reverse.tunnel[0].remoteKey		Optional path to master node Private Key for SSH connection as an alternative for remoteUser for reverse tunnel configuration
xtam.reverse.tunnel[0].forwardHost		Session manager host in the isolated network in the local isolated network space for reverse tunnel configuration
xtam.reverse.tunnel[0].forwardPortLocal		Session manager port in the isolated network for reverse tunnel configuration
xtam.reverse.tunnel [0].forwardPortRemote		Session manager port on the master node to use in the proximity group for reverse tunnel configuration
xtam.reverse.tunnel [0].forwardBindingAddress		Binding address on the master node to expose the port to other interfaces
xtam.reverse.tunnel[0].enabled	true	Flag to enable or disable reverse tunnel configuration
xtam.forward.tunnel[0].remoteHost		Master node host for SSH connection for reverse tunnel configuration
xtam.forward.tunnel[0].remotePort		Master node port for SSH connection for reverse tunnel configuration

Property	Default	Description
xtam.forward.tunnel[0].remoteUser		Master node user for SSH connection for reverse tunnel configuration
xtam.forward.tunnel[0].remotePassword		Master node user password or Private Key password for SSH connection for reverse tunnel configuration
xtam.forward.tunnel[0].remoteKey		Optional path to master node Private Key for SSH connection as an alternative for remoteUser for reverse tunnel configuration
xtam.forward.tunnel[0].forwardHost		Host in the master node network to forward tunnel to
xtam.forward.tunnel[0].forwardPortLocal		Forwarded port on the remote node to map as a master node port
xtam.forward.tunnel [0].forwardPortRemote		Master node port to forward traffic to
xtam.forward.tunnel [0].forwardBindingAddress		Binding address on the remote node to expose the port to other interfaces
xtam.forward.tunnel[0].enabled	true	Flag to enable or disable forward tunnel configuration
xtam.ssh.proxy.banner		SSH Proxy banner to override banner defined in the system parameter
xtam.job.selfCheckStatus	false	This parameter makes Check Status job execution to run by the account on record instead of the shadow account
xtam.session.web.audio	false	Enables audio channel support for WEB Sessions
xtam.replication.sequence		Indicator of node sequence in multi-node High Availability setup. The parameter is given in the form of sequence/total where the sequence (1, 2, 3, …) is the sequence of the node in HA cluster and total is the total number of nodes in the cluster. Among other options, the node will only send notifications about event generated by this node to avoid duplication of alerts.

Property	Default	Description
xtam.ssh.proxy.auth.rest	false	Flag indicating whether SSH Proxy user authentication should fall back to REST authentication after failed attempts to authenticate using integrated LDAP directories.
xtam.web.version.disable	false	Flag disabling automatic version check by the WEB GUI
xtam.export.page.size	500	Page size for export process to control balance between memory consumption and speed of system export
xtam.api.config.check_groups.threads_per_request	5	If many proximity groups are configured and users are experiencing slowness when loading the proximity group page, the value of this property can be increased to a number greater than 5. PAM Manager needs to be restarted if this property is updated
xtam.ldap.cert.auto-import	true	Auto-import AD certificates for internal directory service (on replication) and AD records (on periodical jobs when using LDAPS connection)
xtam.web.cert.auto-import	true	CAS certificate auto import performed on application startup if set to true, disabled if false

System properties reference guide (docx)