[MS-ASPROV]:
ActiveSync Provisioning Protocol Specification

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation for protocols, file formats, languages, standards as well as overviews of the interaction among each of these technologies.
- **Copyrights.** This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you may make copies of it in order to develop implementations of the technologies described in the Open Specifications and may distribute portions of it in your implementations using these technologies or your documentation as necessary to properly document the implementation. You may also distribute in your implementation, with or without modification, any schema, IDL's, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.
- **Patents.** Microsoft has patents that may cover your implementations of the technologies described in the Open Specifications. Neither this notice nor Microsoft's delivery of the documentation grants any licenses under those or any other Microsoft patents. However, a given Open Specification may be covered by Microsoft's Open Specification Promise (available here: http://www.microsoft.com/interop/osp) or the Community Promise (available here: http://www.microsoft.com/interop/cp/default.mspx). If you would prefer a written license, or if the technologies described in the Open Specifications are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting iplg@microsoft.com.
- **Trademarks.** The names of companies and products contained in this documentation may be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights.
- **Fictitious Names.** The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

Reservation of Rights. All other rights are reserved, and this notice does not grant any rights other than specifically described above, whether by implication, estoppel, or otherwise.

Tools. The Open Specifications do not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments you are free to take advantage of them. Certain Open Specifications are intended for use in conjunction with publicly available standard specifications and network programming art, and assumes that the reader either is familiar with the aforementioned material or has immediate access to it.

Revision Summary

Date	Revision History	Revision Class	Comments
12/03/2008	1.0.0	Major	Initial Release.
03/04/2009	1.0.1	Editorial	Revised and edited technical content.
04/10/2009	2.0.0	Major	Updated technical content and applicable product releases.
07/15/2009	3.0.0	Major	Revised and edited for technical content.
11/04/2009	3.1.0	Minor	Updated the technical content.
02/10/2010	3.1.0	None	Version 3.1.0 Release

Table of Contents

1 Introduction

The ActiveSync Provisioning protocol specifies an **XML-based** format that Microsoft Exchange servers use to communicate security policy settings to client devices.

1.1 Glossary

The following terms are defined in [MS-OXGLOS]:

attachment
calendar
collection
condition
encrypted S/MIME messages
header
Hypertext Markup Language (HTML)
Hypertext Transfer Protocol (HTTP)
message
MIME message
permissions
plain text
series
Short Message Service (SMS)
state
storage
store
synchronization
Uniform Resource Identifier (URI)
WAP Binary XML (WBXML)
XML
XML schema

The following terms are specific to this document:

policy key: A stored value that represents the state of a policy or setting.

remote wipe: Functionality that is implemented on a client, initiated by policy or a request from a server, that requires the client to delete all data and settings related to the referenced protocol.

MAY, SHOULD, MUST, SHOULD NOT, MUST NOT: These terms (in all caps) are used as described in [RFC2119]. All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

1.2 References

1.2.1 Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact dochelp@microsoft.com. We will assist you in finding the relevant information. Please check the archive site, http://msdn2.microsoft.com/en-us/library/E4BD6494-06AD-4aed-9823-445E921C9624, as an additional source.

[MS-ASAIRS] Microsoft Corporation, "ActiveSync AirSyncBase Namespace Protocol Specification", December 2008.

[MS-ASCMD] Microsoft Corporation, "ActiveSync Command Reference Protocol Specification", December 2008.

[MS-ASDOC] Microsoft Corporation, "ActiveSync Document Class Protocol Specification", December 2008.

[MS-ASDTYPE] Microsoft Corporation, "ActiveSync Data Types", December 2008.

[MS-ASWBXML] Microsoft Corporation, "ActiveSync WAP Binary XML (WBXML) Protocol Specification", December 2008.

[MS-OXGLOS] Microsoft Corporation, "Exchange Server Protocols Master Glossary", June 2008.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, http://www.ietf.org/rfc/rfc2119.txt.

1.2.2 Informative References

None.

1.3 Protocol Overview

The Provisioning protocol consists of an **XML schema** that defines the elements that are necessary for an ActiveSync device to specify its capabilities and **permissions**.

1.4 Relationship to Other Protocols

The document class protocol [MS-ASDOC] specifies the XML format that is used by the **Provision** command, as specified in [MS-ASCMD].

All simple data types in this document conform to the data type definitions specified in [MS-ASDTYPE].

1.5 Prerequisites/Preconditions

None.

1.6 Applicability Statement

None.

1.7 Versioning and Capability Negotiation

None.

1.8 Vendor-Extensible Fields

None.

1.9 Standards Assignments

None.

2 Messages

2.1 Transport

The ActiveSync Provisioning protocol consists of a **series** of XML elements that are embedded within a request or response that is associated with the **Provision** command, as specified in [MS-ASCMD].

2.2 Message Syntax

The XML markup that constitutes the Request Body or the Response Body is transmitted between client and server by using **WAP Binary XML (WBXML)**. For details, see [MS-ASWBXML].

The following is the XML schema definition for the ActiveSync Provisioning protocol.

```
<?xml version="1.0" ?>
<xs:schema xmlns:tns="Provision:" attributeFormDefault="unqualified"
elementFormDefault="qualified"      targetNamespace="Provision:"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:element name="Provision">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="Status" type="unsignedByte" />
             <xs:element name="Policies">
                 <xs:complexType>
                     <xs:sequence>
                         <xs:element name="Policy">
                             <xs:complexType>
                                 <xs:sequence>
                                     <xs:element name="PolicyType" type="xs:string" />
                                     <xs:element name="Status" type="xs:unsignedByte" />
                                     <xs:element name="PolicyKey" type="xs:string" />
                                     <xs:element name="Data">
                                         <xs:complexType>
                                           <xs:sequence>
                                             <xs:element name="eas-provisioningdoc">
                                               <xs:complexType>
                                                 <xs:sequence>
                                                   <xs:element name="DevicePasswordEnabled"
type="xs:unsignedByte" />
                                                   <xs:element
name="AlphaNumericDevicePasswordRequired" type="xs:unsignedByte" />
                                                   <xs:element name="PasswordRecoveryEnabled"
type="xs:unsignedByte" />
                                                   <xs:element name="DeviceEncryptionEnabled"
type="xs:unsignedByte" />
                                                   <xs:element name="AttachmentsEnabled"
type="xs:unsignedByte" />
                                                   <xs:element name="MinDevicePasswordLength"
type="xs:unsignedByte" />
                                                   <xs:element
name="MaxInactivityTimeDeviceLock" type="xs:unsignedByte" />
                                                   <xs:element
name="MaxDevicePasswordFailedAttempts" tpe="xs:unsignedByte" />
                                                   <xs:element name="MaxAttachmentSize" />
                                                   <xs:element
name="AllowSimpleDevicePassword" type="xs:unsignedByte" />
                                                   <xs:element
name="DevicePasswordExpiration" />
```

```
                                                <xs:element name="DevicePasswordHistory"
type="xs:unsignedByte" />
                                                <xs:element name="AllowStorageCard"
type="xs:unsignedByte" />
                                                <xs:element name="AllowCamera"
type="xs:unsignedByte" />
                                                <xs:element name="RequireDeviceEncryption"
type="xs:unsignedByte" />
                                                <xs:element
name="RequireStorageCardEncryption" type="xs:unsignedByte" />
                                                <xs:element
name="AllowUnsignedApplications" type="xs:unsignedByte" />
                                                <xs:element
name="AllowUnsignedInstallationPackages" type="xs:unsignedByte" />
                                                <xs:element
name="MinDevicePasswordComplexCharacters" type="xs:unsignedByte" />
                                                <xs:element name="AllowWiFi"
type="xs:unsignedByte" />
                                                <xs:element name="AllowTextMessaging"
type="xs:unsignedByte" />
                                                <xs:element name="AllowPOPIMAPEmail"
type="xs:unsignedByte" />
                                                <xs:element name="AllowBluetooth"
type="xs:unsignedByte" />
                                                <xs:element name="AllowIrDA"
type="xs:unsignedByte" />
                                                <xs:element
name="RequireManualSyncWhenRoaming" type="xs:unsignedByte" />
                                                <xs:element name="AllowDesktopSync"
type="xs:unsignedByte" />
                                                <xs:element name="MaxCalendarAgeFilter"
type="xs:unsignedByte" />
                                                <xs:element name="AllowHTMLEmail"
type="xs:unsignedByte" />
                                                <xs:element name="MaxEmailAgeFilter"
type="xs:unsignedByte" />
                                                <xs:element
name="MaxEmailBodyTruncationSize" type="xs:unsignedByte" />
                                                <xs:element
name="MaxEmailHTMLBodyTruncationSize" type="xs:unsignedByte" />
                                                <xs:element
name="RequireSignedSMIMEMessages" type="xs:unsignedByte" />
                                                <xs:element
name="RequireEncryptedSMIMEMessages " type="xs:unsignedByte" />
                                                <xs:element
name="RequireSignedSMIMEAlgorithm" type="xs:unsignedByte" />
                                                <xs:element
name="RequireEncryptionSMIMEAlgorithm" type="xs:unsignedByte" />
                                                <xs:element
name="AllowSMIMEEncryptionAlgorithmNegotiation" type="xs:unsignedByte" />
                                                <xs:element name="AllowSMIMESoftCerts"
type="xs:unsignedByte" />
                                                <xs:element name="AllowBrowser"
type="xs:unsignedByte" />
                                                <xs:element name="AllowConsumerEmail"
type="xs:unsignedByte" />
                                                <xs:element name="AllowRemoteDesktop"
type="xs:unsignedByte" />
                                                <xs:element name="AllowInternetSharing"
type="xs:unsignedByte" />
                                                <xs:element
name="UnapprovedInROMApplicationList">
```

```
                                                    <xs:complexType>
                                                        <xs:sequence>
                                                            <xs:element
name="ApplicationName" type="xs:string" />
                                                        </xs:sequence>
                                                    </xs:complexType>
                                                </xs:element>
                                                <xs:element
name="ApprovedApplicationList">
                                                    <xs:complexType>
                                                        <xs:sequence>
                                                            <xs:element name="Hash"
type="xs:string" />
                                                        </xs:sequence>
                                                    </xs:complexType>
                                                </xs:element>
                                            </xs:sequence>
                                        </xs:complexType>
                                    </xs:element>
                                </xs:sequence>
                            </xs:complexType>
                        </xs:element>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
</xs:element>

</xs:schema>
```

This specification defines and references the following XML namespace.

Prefix	Reference
Provision:	[MS-ASPROV]

2.2.1 Complex Types

The following table summarizes the set of common XML schema complex type definitions defined by this specification.

Complex Type	Description
Policies	A **collection** of security policies.
Policies.Policy	A policy.
Policies.Policy.Data	The settings for a policy.
Policies.Policy.Data.eas-provisioningdoc	The collection of security settings for device provisioning.
Policies.Policy.Data.eas-	A list of in-ROM applications that are not

Complex Type	Description
provisioningdoc.UnapprovedInROMApplicationList	approved for execution.
Policies.Policy.Data.eas-provisioningdoc.ApprovedApplicationList	A list of in-RAM applications that are approved for execution.

2.2.1.1 Policies

The **Policies** type is a required **container** ([MS-ASDTYPE] section 2.8) type that specifies a collection of security policies.

A command response has one top-level **Policies** type per response.

The **Policies** type has only the following child element:

- **Policy** (section 2.2.1.2): At least one element of this type is required.

2.2.1.2 Policies.Policy

The **Policies.Policy** type is a required **container** ([MS-ASDTYPE] section 2.8) type that specifies a policy.

This element is only valid in a command response.

The **Policies.Policy** type has only the following child elements:

- <Policies.Policy.PolicyType> (section 2.2.2.2)
- <Policies.Policy.Status> (section 2.2.2.3)
- <Policies.Policy.PolicyKey> (section 2.2.2.4)
- **Policies.Policy.Data** (section 2.2.1.3): One instance of this element is required.

2.2.1.3 Policies.Policy.Data

The **Policies.Policy.Data** type is a required **container** ([MS-ASDTYPE] section 2.8) type that specifies the settings for a policy.

The **Policies.Policy.Data** type has only the following child element:

- **Policies.Policy.Data.eas-provisioningdoc** (section 2.2.1.4): One instance of this element is required.

2.2.1.4 Policies.Policy.Data.eas-provisioningdoc

The <Policies.Policy.Data.eas-provisioningdoc> element is a required **container** ([MS-ASDTYPE] section 2.8) element that specifies the collection of security settings for device provisioning.

A command response has a minimum of one <Policies.Policy.Data.eas-provisioningdoc> type per <Policies.Policy.Data> element.

The <Policies.Policy.Data.eas-provisioningdoc> type has only the following child elements:

- <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled> (section 2.2.2.5)

- <Policies.Policy.Data.eas-provisioningdoc.AlphaNumericDevicePasswordRequired> (section 2.2.2.6)
- <Policies.Policy.Data.eas-provisioningdoc.PasswordRecoveryEnabled> (section 2.2.2.7)
- <Policies.Policy.Data.eas-provisioningdoc.DeviceEncryptionEnabled> (section 2.2.2.8)
- <Policies.Policy.Data.eas-provisioningdoc.AttachmentsEnabled> (section 2.2.2.9)
- <Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordLength> (section 2.2.2.10)
- <Policies.Policy.Data.eas-provisioningdoc.MaxInactivityTimeDeviceLock> (section 2.2.2.11)
- <Policies.Policy.Data.eas-provisioningdoc.MaxDevicePasswordFailedAttempts> (section 2.2.2.12)
- <Policies.Policy.Data.eas-provisioningdoc.MaxAttachmentSize> (section 2.2.2.13)
- <Policies.Policy.Data.eas-provisioningdoc.AllowSimpleDevicePassword> (section 2.2.2.14)
- <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordExpiration> (section 2.2.2.15)
- <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordHistory> (section 2.2.2.16)
- <Policies.Policy.Data.eas-provisioningdoc.AllowStorageCard> (section 2.2.2.17)
- <Policies.Policy.Data.eas-provisioningdoc.AllowCamera> (section 2.2.2.18)
- <Policies.Policy.Data.eas-provisioningdoc.RequireDeviceEncryption> (section 2.2.2.19)
- <Policies.Policy.Data.eas-provisioningdoc.RequireStorageCardEncryption> (section 2.2.2.20)
- <Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedApplications> (section 2.2.2.21)
- <Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedInstallationPackages> (section 2.2.2.22)
- <Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordComplexCharacters> (section 2.2.2.23)
- <Policies.Policy.Data.eas-provisioningdoc.AllowWifi> (section 2.2.2.24)
- <Policies.Policy.Data.eas-provisioningdoc.AllowTextMessaging> (section 2.2.2.25)
- <Policies.Policy.Data.eas-provisioningdoc.AllowPOPIMAPEmail> (section 2.2.2.26)
- <Policies.Policy.Data.eas-provisioningdoc.AllowBluetooth> (section 2.2.2.27)
- <Policies.Policy.Data.eas-provisioningdoc.AllowIrDA> (section 2.2.2.28)
- <Policies.Policy.Data.eas-provisioningdoc.RequireManualSyncWhenRoaming> (section 2.2.2.29)
- <Policies.Policy.Data.eas-provisioningdoc.AllowDesktopSync> (section 2.2.2.30)
- <Policies.Policy.Data.eas-provisioningdoc.MaxCalendarAgeFilter> (section 2.2.2.31)
- <Policies.Policy.Data.eas-provisioningdoc.AllowHTMLEmail> (section 2.2.2.32)
- <Policies.Policy.Data.eas-provisioningdoc.MaxEmailAgeFilter> (section 2.2.2.33)
- <Policies.Policy.Data.eas-provisioningdoc.MaxEmailBodyTruncationSize> (section 2.2.2.34)

- <Policies.Policy.Data.eas-provisioningdoc.MaxEmailHTMLBodyTruncationSize> (section 2.2.2.35)
- <Policies.Policy.Data.eas-provisioningdoc.RequireSignedSMIMEMessages> (section 2.2.2.36)
- <Policies.Policy.Data.eas-provisioningdoc.RequireEncryptedSMIMEMessages> (section 2.2.2.37)
- <Policies.Policy.Data.eas-provisioningdoc.RequireSignedSMIMEAlgorithm> (section 2.2.2.38)
- <Policies.Policy.Data.eas-provisioningdoc.RequireEncryptionSMIMEAlgorithm> (section 2.2.2.39)
- <Policies.Policy.Data.eas-provisioningdoc.AllowSMIMEEncryptionAlgorithmNegotiation> (section 2.2.2.40)
- <Policies.Policy.Data.eas-provisioningdoc.AllowSMIMESoftCerts> (section 2.2.2.41)
- <Policies.Policy.Data.eas-provisioningdoc.AllowBrowser> (section 2.2.2.42)
- <Policies.Policy.Data.eas-provisioningdoc.AllowConsumerEmail> (section 2.2.2.43)
- <Policies.Policy.Data.eas-provisioningdoc.AllowRemoteDesktop> (section 2.2.2.44)
- <Policies.Policy.Data.eas-provisioningdoc.AllowInternetSharing> (section 2.2.2.45)

2.2.1.5 Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList

The **Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList** type is an optional **container** ([MS-ASDTYPE] section 2.8) element that specifies a list of in-ROM applications that are not approved for execution.

A command response has a maximum of one **Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList** type per **Policies.Policy.Data.eas-provisioningdoc** type.

The **Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList** type has only the following child elements:

- <Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList.ApplicationName> (Section 2.2.2.46): At least one instance of this element is required.

2.2.1.6 Policies.Policy.Data.eas-provisioningdoc.ApprovedApplicationList

The **Policies.Policy.Data.eas-provisioningdoc.ApprovedApplicationList** element is an optional **container** ([MS-ASDTYPE] section 2.8) element that specifies a list of in-memory applications that are approved for execution.

A command response has a maximum of one **Policies.Policy.Data.eas-provisioningdoc.ApprovedApplicationList** type per <Policies.Policy.Data.eas-provisioningdoc> element.

The **Policies.Policy.Data.eas-provisioningdoc.ApprovedApplicationList** type has only the following child elements:

- <Policies.Policy.Data.eas-provisioningdoc.ApprovedApplicationList.Hash> (section 2.2.2.47): At least one instance of this element is required.

2.2.2 Elements

The following table summarizes the set of common XML schema element definitions that are defined or used by this specification. XML schema elements that are specific to a particular command are described in the context of its associated command.

Element	Description
<Status>	Indicates whether the **Provision** command was handled correctly.
<Policies.Policy.PolicyType>	Specifies the format in which the policy settings are to be provided.
<Policies.Policy.Status>	Indicates whether the policy settings were applied correctly.
<Policies.Policy.PolicyKey>	Used by the server to mark the **state** of policy settings on the client.
<Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled>	Indicates whether a client device requires a password.
<Policies.Policy.Data.eas-provisioningdoc.AlphaNumericDevicePasswordRequired>	Indicates whether a client device requires an AlphaNumeric password.
<Policies.Policy.Data.eas-provisioningdoc.PasswordRecoveryEnabled>	Indicates whether to enable a recovery password to be sent to the server by using the **Settings** command.
<Policies.Policy.Data.eas-provisioningdoc.DeviceEncryptionEnabled>	Indicates whether the device has to encrypt content that is stored on the **storage** card.
<Policies.Policy.Data.eas-provisioningdoc.AttachmentsEnabled>	Indicates whether e-mail **attachments** are enabled.
<Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordLength>	The minimum device password length that the user can enter.
<Policies.Policy.Data.eas-provisioningdoc.MaxInactivityTimeDeviceLock>	The number of seconds of inactivity before the device locks itself.
<Policies.Policy.Data.eas-provisioningdoc.MaxDevicePasswordFailedAttempts>	The number of password failures that are permitted before the device is wiped.
<Policies.Policy.Data.eas-provisioningdoc.MaxAttachmentSize>	The maximum attachment size, as determined by the security policy.
<Policies.Policy.Data.eas-provisioningdoc.AllowSimpleDevicePassword>	Whether the device allows simple passwords.

Element	Description
<Policies.Policy.Data.eas-provisioningdoc.DevicePasswordExpiration>	Whether the password expires, as determined by the policy.
<Policies.Policy.Data.eas-provisioningdoc.DevicePasswordHistory>	Whether the device **stores** the history of the password.
<Policies.Policy.Data.eas-provisioningdoc.AllowStorageCard>	Whether the device allows the use of the storage card.
<Policies.Policy.Data.eas-provisioningdoc.AllowCamera>	Whether the device allows the use of the built-in camera.
<Policies.Policy.Data.eas-provisioningdoc.RequireStorageCardEncryption>	Whether the device encrypts content that is stored on the storage card.
<Policies.Policy.Data.eas-provisioningdoc.RequireDeviceEncryption>	Whether the device uses encryption.
<Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedApplications>	Whether the device allows unsigned applications to execute.
<Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedInstallationPackages>	Whether the device allows unsigned CAB files to be installed.
<Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordComplexCharacters>	The minimum number of complex characters (numbers and symbols) contained within the password.
<Policies.Policy.Data.eas-provisioningdoc.AllowWiFi>	Whether the device allows the use of WiFi connections.
<Policies.Policy.Data.eas-provisioningdoc.AllowTextMessaging>	Whether the device allows **SMS**/text messaging.
<Policies.Policy.Data.eas-provisioningdoc.AllowPOPIMAPEmail>	Whether the device allows access to POP/IMAP e-mail.
<Policies.Policy.Data.eas-provisioningdoc.AllowBluetooth>	Whether Bluetooth and hands-free profiles are allowed on the device.
<Policies.Policy.Data.eas-provisioningdoc.AllowIrDA>	Whether the device allows the use of IrDA (infrared) connections.
<Policies.Policy.Data.eas-provisioningdoc.RequireManualSyncWhenRoaming>	Whether the device requires manual **synchronization** when the device is roaming.
<Policies.Policy.Data.eas-provisioningdoc.AllowDesktopSync>	Whether the device allows synchronization with Desktop ActiveSync.
<Policies.Policy.Data.eas-provisioningdoc.MaxCalendarAgeFilter>	The maximum number of

Element	Description
	calendar days that can be synchronized.
<Policies.Policy.Data.eas-provisioningdoc.AllowHTMLEmail>	Whether the device uses **HTML**-formatted e-mail.
<Policies.Policy.Data.eas-provisioningdoc.MaxEmailAgeFilter>	The e-mail age limit for synchronization.
<Policies.Policy.Data.eas-provisioningdoc.MaxEmailBodyTruncationSize>	The truncation size for **plain text**–formatted e-mail **messages**.
<Policies.Policy.Data.eas-provisioningdoc.MaxEmailHTMLBodyTruncationSize>	The truncation size for HTML-formatted e-mail messages.
<Policies.Policy.Data.eas-provisioningdoc.RequireSignedSMIMEMessages>	Whether the device is required to send signed S/**MIME messages**.
<Policies.Policy.Data.eas-provisioningdoc.RequireEncryptedSMIMEMessages>	Whether the device is required to send **encrypted S/MIME messages**.
<Policies.Policy.Data.eas-provisioningdoc.RequireSignedSMIMEAlgorithm>	The algorithm to be used when signing a message.
<Policies.Policy.Data.eas-provisioningdoc.RequireEncryptionSMIMEAlgorithm>	The algorithm to be used when encrypting a message.
<Policies.Policy.Data.eas-provisioningdoc.AllowSMIMEEncryptionAlgorithmNegotiation>	Whether the device can negotiate the encryption algorithm to be used for signing.
<Policies.Policy.Data.eas-provisioningdoc.AllowSMIMESoftCerts>	Whether the device uses soft certificates to sign outgoing messages.
<Policies.Policy.Data.eas-provisioningdoc.AllowBrowser>	Whether the device allows the use of a web browser.
<Policies.Policy.Data.eas-provisioningdoc.AllowConsumerEmail>	Whether the device allows the use of Windows Live.
<Policies.Policy.Data.eas-provisioningdoc.AllowRemoteDesktop>	Whether the device allows the use of Remote Desktop.
<Policies.Policy.Data.eas-provisioningdoc.AllowInternetSharing>	Whether the device allows the use of Internet Sharing.
<Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList.ApplicationName>	The name of an in-ROM application (.exe file) that is not approved for execution.
<Policies.Policy.Data.eas-provisioningdoc.ApprovedApplicationList.Hash>	The SHA-1 hash of an in-memory application that is approved for execution.

2.2.2.1 Status

The <Status> element indicates success of the command in two different locations in the response. The <Status> element that is returned as a direct child of the <Provision> element indicates whether the **Provision** command was handled correctly.

The following table lists valid values for the <Status> element.

Value	Meaning
1	Success
2	Protocol error
3	General server error
4	The device is externally managed

2.2.2.2 Policies.Policy.PolicyType

In the download policy settings phase, the <PolicyType> element specifies the format in which the policy settings are to be provided to the client device.

<PolicyType> MUST be MS-EAS-Provisioning-WBXML.

2.2.2.3 Policies.Policy.Status

The <Status> element indicates success of the command in two different locations in the response. The <Status> element that is returned as a child of a <Status> element indicates whether the policy settings were applied correctly.

The following table lists valid values for the <Status> element as a child of the <Status> element in the response from the server to the client.

Value	Meaning
1	Success.
2	There is no policy for this client.
3	Unknown <PolicyType> value.
4	The policy data on the server is corrupted (possibly tampered with).
5	The client is acknowledging the wrong **policy key**.

The following table lists valid values for the <Status> element as a child of the <Policy> element in the response from the client to the server.

Value	Meaning
1	Success
2	Partial success (at least the PIN was enabled).
3	The client did not apply the policy at all.

Value	Meaning
4	The client claims to have been provisioned by a third party.

2.2.2.4 Policies.Policy.PolicyKey

<PolicyKey> is an optional element of type **string** with a maximum of 64 characters and no child elements.

<PolicyKey> is used by the server to mark the state of policy settings on the client in the settings download phase of the **Provision** command. In the acknowledgement phase, the <PolicyKey> element is used by the client and server to correlate acknowledgements to a particular policy setting.

The <PolicyKey> element is a random unique unsigned **integer**. When the client issues an initial **Provision** command, the <PolicyKey> tag and X-MS-PolicyKey is not included in the **HTTP header**.

2.2.2.5 Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled

The <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled> element is a child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether a device requires a password.

The **Policies.Policy.Data.eas-provisioningdoc** type has at least one **instance** of the <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled> element.

The **Policies.Policy.Data.eas-provisioningdoc** type has either 0 (zero) or 1 instance of the <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled> element.

The <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled> are listed in the following table.

Value	Description
0	Device password is not enabled.
1	Device password is enabled.

2.2.2.6 Policies.Policy.Data.eas-provisioningdoc.AlphaNumericDevicePasswordRequired

The <Policies.Policy.Data.eas-provisioningdoc.AlphaNumericDevicePasswordRequired> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether a device requires an alphanumeric password.

The **Policies.Policy.Data.eas-provisioningdoc** type has either 0 (zero) or 1 instance of the <Policies.Policy.Data.eas-provisioningdoc.AlphaNumericDevicePasswordRequired> element.

The <Policies.Policy.Data.eas-provisioningdoc.AlphaNumericDevicePasswordRequired> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AlphaNumericDevicePasswordRequired> are listed in the following table.

Value	Description
0	Alphanumeric device password is not enabled.
1	Alphanumeric device password is enabled.

If Policies.Policy.Data.eas-provisioningdoc.AlphaNumericDevicePasswordRequired> is not included in a response a client SHOULD treat this value as 0.

If the <Policies.Policy.Data.eas-provisioningdoc.AlphaNumericDevicePasswordRequired> element is included in a response, and <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled> is FALSE (0), the client ignores this element.

2.2.2.7 Policies.Policy.Data.eas-provisioningdoc.PasswordRecoveryEnabled

The <Policies.Policy.Data.eas-provisioningdoc.PasswordRecoveryEnabled> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether to enable a recovery password to be sent to the server by using the **Settings** command.

The **Policies.Policy.Data.eas-provisioningdoc** type has either 0 (zero) or 1 instance of the <Policies.Policy.Data.eas-provisioningdoc.PasswordRecoveryEnabled> element.

The <Policies.Policy.Data.eas-provisioningdoc.PasswordRecoveryEnabled> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.PasswordRecoveryEnabled> are listed in the following table.

Value	Description
0	Password recovery is not enabled.
1	Password recovery is enabled.

A recovery password is a password that is created by the device that gives the administrator or user the ability to log on to the device one time, using the recovery password, after which time the user is forced to create a new password. The device then creates a new recovery password. If this element is set to 1 (TRUE), the device can send a password, but the server does not enforce the policy. If the element is set to 0 (FALSE), the device SHOULD NOT send a recovery password, because the server will refuse to store the password.

If Policies.Policy.Data.eas-provisioningdoc.PasswordRecoveryEnabled> is not included in a response a client SHOULD treat this value as 0.

If the <Policies.Policy.Data.eas-provisioningdoc.PasswordRecoveryEnabled> element is included in a response, and <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled> is FALSE (0), the client SHOULD ignore this element.

2.2.2.8 Policies.Policy.Data.eas-provisioningdoc.DeviceEncryptionEnabled

The <Policies.Policy.Data.eas-provisioningdoc.DeviceEncryptionEnabled> element is a child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device encrypts content that is stored on the storage card.

The **Policies.Policy.Data.eas-provisioningdoc** type has either 0 (zero) or 1instance of the <Policies.Policy.Data.eas-provisioningdoc.DeviceEncryptionEnabled> element.

The <Policies.Policy.Data.eas-provisioningdoc.DeviceEncryptionEnabled> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.DeviceEncryptionEnabled> are listed in the following table.

Value	Description
0	Device encryption is not enabled.
1	Device encryption is enabled.

2.2.2.9 Policies.Policy.Data.eas-provisioningdoc.AttachmentsEnabled

The <Policies.Policy.Data.eas-provisioningdoc.AttachmentsEnabled> element is a child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether e-mail attachments are enabled.

The **Policies.Policy.Data.eas-provisioningdoc** type has either 0 (zero) or 1 instance of the <Policies.Policy.Data.eas-provisioningdoc.AttachmentsEnabled> element.

The <Policies.Policy.Data.eas-provisioningdoc.AttachmentsEnabled> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AttachmentsEnabled> are listed in the following table.

Value	Description
0	attachments are not enabled.
1	attachments are enabled.

2.2.2.10 Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordLength

The <Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordLength> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies the minimum device password length that the user can enter.

The **Policies.Policy.Data.eas-provisioningdoc** type has either 0 (zero) or 1 instance of the <Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordLength> element.

The <Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordLength> element cannot have child elements.

<Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordLength> is an **integer**. <Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordLength> MUST have a value no less than 1 and no greater than 16. If the value of this element is 1, there is no minimum length for the device password.

If the <Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordLength> element is included in a response, and **Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled** is FALSE (0), the client SHOULD ignore this element.

2.2.2.11 Policies.Policy.Data.eas-provisioningdoc.MaxInactivityTimeDeviceLock

The <Policies.Policy.Data.eas-provisioningdoc.MaxInactivityTimeDeviceLock> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies the number of seconds of inactivity before the device locks itself.

The **Policies.Policy.Data.eas-provisioningdoc** type has 0 (zero) or 1 instance of the <Policies.Policy.Data.eas-provisioningdoc.MaxInactivityTimeDeviceLock> element.

The <Policies.Policy.Data.eas-provisioningdoc.MaxInactivityTimeDeviceLock> element cannot have child elements.

<Policies.Policy.Data.eas-provisioningdoc.MaxInactivityTimeDeviceLock> is an **integer**. If this value is greater than or equal to 9999, the client interprets it as 0.

If the <Policies.Policy.Data.eas-provisioningdoc.MaxInactivityTimeDeviceLock> element is not included in a response, the client interprets this as meaning that no time device lock has been set by the security policy.

2.2.2.12 Policies.Policy.Data.eas-provisioningdoc.MaxDevicePasswordFailedAttempts

The <Policies.Policy.Data.eas-provisioningdoc.MaxDevicePasswordFailedAttempts> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies the number of password logon attempts that are permitted before the device locks itself.

The **Policies.Policy.Data.eas-provisioningdoc** type has 0 (zero) or 1 instance of the <Policies.Policy.Data.eas-provisioningdoc.MaxDevicePasswordFailedAttempts> element.

The <Policies.Policy.Data.eas-provisioningdoc.MaxDevicePasswordFailedAttempts> element cannot have child elements.

<Policies.Policy.Data.eas-provisioningdoc.MaxDevicePasswordFailedAttempts> is an **integer** with a value of no less than 2 and no greater than 4294967295.

If the <Policies.Policy.Data.eas-provisioningdoc.MaxDevicePasswordFailedAttempts> element is included in a response, and the <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled> element is set to FALSE (0), the client ignores this element.

2.2.2.13 Policies.Policy.Data.eas-provisioningdoc.MaxAttachmentSize

The <Policies.Policy.Data.eas-provisioningdoc.MaxAttachmentSize> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies the maximum attachment size as determined by security policy.

The **Policies.Policy.Data.eas-provisioningdoc** type has at least one instance of the <Policies.Policy.Data.eas-provisioningdoc.MaxAttachmentSize> element.

The **Policies.Policy.Data.eas-provisioningdoc** type has 0 (zero) or 1 instance of the <Policies.Policy.Data.eas-provisioningdoc.MaxAttachmentSize> element.

The <Policies.Policy.Data.eas-provisioningdoc.MaxAttachmentSize> element cannot have child elements.

<Policies.Policy.Data.eas-provisioningdoc.MaxAttachmentSize> is an **integer**.

2.2.2.14 Policies.Policy.Data.eas-provisioningdoc.AllowSimpleDevicePassword

The <Policies.Policy.Data.eas-provisioningdoc.AllowSimpleDevicePassword> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device allows simple passwords. A simple password is one with digits only (integers 0-9).

The **Policies.Policy.Data.eas-provisioningdoc** type has 0 (zero) or 1 instance of the <Policies.Policy.Data.eas-provisioningdoc.AllowSimpleDevicePassword> element.

The <Policies.Policy.Data.eas-provisioningdoc.AllowSimpleDevicePassword> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowSimpleDevicePassword> are listed in the following table.

Value	Description
0	Simple passwords are not allowed.
1	Simple passwords are allowed.

If Policies.Policy.Data.eas-provisioningdoc.AllowSimpleDevicePassword> is not included in a response a client SHOULD treat this value as 0.

If the <Policies.Policy.Data.eas-provisioningdoc.AllowSimpleDevicePassword> element is included in a response, and the <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled> element is set to FALSE (0), the client ignores this element.

2.2.2.15 Policies.Policy.Data.eas-provisioningdoc.DevicePasswordExpiration

The <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordExpiration> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the password expires.

The **Policies.Policy.Data.eas-provisioningdoc** type has 0 (zero) or 1 instance of the <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordExpiration> element.

The <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordExpiration> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordExpiration> are listed in the following table.

Value	Description
0	Passwords do not expire.
1	Passwords expire.

If Policies.Policy.Data.eas-provisioningdoc.DevicePasswordExpiration> is not included in a response a client SHOULD treat this value as 0.

If the <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordExpiration> element is included in a response, and the <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled> element is set to FALSE (0), then the client ignores this element.

2.2.2.16 Policies.Policy.Data.eas-provisioningdoc.DevicePasswordHistory

The <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordHistory> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device stores previously used passwords.

The **Policies.Policy.Data.eas-provisioningdoc** type has either 0 (zero) or 1 instance of the <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordHistory> element.

The <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordHistory> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordHistory> are listed in the following table.

Value	Description
0	Previously used passwords are not stored.
1	Previously used passwords are stored.

If <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordHistory> is not included in a response, then a client SHOULD treat this value as 0.

If the value of the <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordHistory> element is set to TRUE (1), and the value of the <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled> element is also set to TRUE (1), the client disallows the user from using a prior password after a password expires.

If the <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordHistory> element is included in a response, and the <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled> element is set to FALSE (0), the client ignores this element. Similarly, if the <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled> element is set to FALSE (0) or is not included in the response, the client also ignores this element.

2.2.2.17 Policies.Policy.Data.eas-provisioningdoc.AllowStorageCard

The <Policies.Policy.Data.eas-provisioningdoc.AllowStorageCard> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device allows use of the storage card.

The **Policies.Policy.Data.eas-provisioningdoc** type has at least one instance of the <Policies.Policy.Data.eas-provisioningdoc.AllowStorageCard> element.

The **Policies.Policy.Data.eas-provisioningdoc** type has either 0 (zero) or 1 instance of the <Policies.Policy.Data.eas-provisioningdoc.AllowStorageCard> element.

The <Policies.Policy.Data.eas-provisioningdoc.AllowStorageCard> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowStorageCard> are listed in the following table.

Value	Description
0	SD card use is not allowed.

Value	Description
1	SD card use is allowed.

2.2.2.18 Policies.Policy.Data.eas-provisioningdoc.AllowCamera

The <Policies.Policy.Data.eas-provisioningdoc.AllowCamera> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device allows the use of the built-in camera.

The **Policies.Policy.Data.eas-provisioningdoc** type has at least one instance of the <Policies.Policy.Data.eas-provisioningdoc.AllowCamera> element.

The **Policies.Policy.Data.eas-provisioningdoc** type has either 0 (zero) or 1 instance of the <Policies.Policy.Data.eas-provisioningdoc.AllowCamera> element.

The <Policies.Policy.Data.eas-provisioningdoc.AllowCamera> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowCamera> are listed in the following table.

Value	Description
0	Use of the camera is not allowed.
1	Use of the camera is allowed.

2.2.2.19 Policies.Policy.Data.eas-provisioningdoc.RequireDeviceEncryption

The <Policies.Policy.Data.eas-provisioningdoc.RequireDeviceEncryption> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device uses encryption.

The **Policies.Policy.Data.eas-provisioningdoc** type has at least one instance of the <Policies.Policy.Data.eas-provisioningdoc.RequireDeviceEncryption> element.

The **Policies.Policy.Data.eas-provisioningdoc** type has either 0 (zero) or 1 instance of the <Policies.Policy.Data.eas-provisioningdoc.RequireDeviceEncryption> element.

The <Policies.Policy.Data.eas-provisioningdoc.RequireDeviceEncryption> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.RequireDeviceEncryption> are listed in the following table.

Value	Description
0	Encryption is not required.
1	Encryption is required.

2.2.2.20 Policies.Policy.Data.eas-provisioningdoc.RequireStorageCardEncryption

The <Policies.Policy.Data.eas-provisioningdoc.RequireStorageCardEncryption> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device encrypts content that is stored on the storage card.

The **Policies.Policy.Data.eas-provisioningdoc** type has either 0 (zero) or 1 instance of the <Policies.Policy.Data.eas-provisioningdoc.RequireStorageCardEncryption> element.

The <Policies.Policy.Data.eas-provisioningdoc.RequireStorageCardEncryption> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.RequireStorageCardEncryption> are listed in the following table.

Value	Description
0	Encryption of storage card contents is not required.
1	Encryption of storage card contents is required.

2.2.2.21 Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedApplications

The <Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedApplications> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device allows unsigned applications to execute.

The **Policies.Policy.Data.eas-provisioningdoc** type has at least one instance of the <Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedApplications> element.

The **Policies.Policy.Data.eas-provisioningdoc** type has either 0 (zero) or 1 instance of the <Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedApplications> element.

The <Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedApplications> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedApplications> are listed in the following table.

Value	Description
0	Unsigned applications are not allowed to execute.
1	Unsigned applications are allowed to execute.

2.2.2.22 Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedInstallationPackages

The <Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedInstallationPackages> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device allows unsigned CAB files to be installed.

The **Policies.Policy.Data.eas-provisioningdoc** type has at least one instance of the <Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedInstallationPackages> element.

The **Policies.Policy.Data.eas-provisioningdoc** type has either 0 (zero) or 1 instance of the <Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedInstallationPackages> element.

The <Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedInstallationPackages> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedInstallationPackages> are listed in the following table.

Value	Description
0	Unsigned CAB files are allowed to be installed.
1	Unsigned CAB files are not allowed to be installed.

2.2.2.23 Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordComplexCharacters

The <Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordComplexCharacters> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies the number of complex characters (numbers and symbols) that the device password must contain. Valid values are 1 through 4.

The **Policies.Policy.Data.eas-provisioningdoc** type has either 0 (zero) or 1 instance of the <Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordComplexCharacters> element.

The <Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordComplexCharacters> element cannot have child elements.

<Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordComplexCharacters> is an **integer**. Valid values for <Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordComplexCharacters> are 1 to 4.

2.2.2.24 Policies.Policy.Data.eas-provisioningdoc.AllowWifi

The <Policies.Policy.Data.eas-provisioningdoc.AllowWifi> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device allows the use of Wi-Fi connections.

The <Policies.Policy.Data.eas-provisioningdoc.AllowWifi> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowWifi> are listed in the following table.

Value	Description
0	The use of Wi-Fi connections is not allowed.
1	The use of Wi-Fi connections is allowed.

2.2.2.25 Policies.Policy.Data.eas-provisioningdoc.AllowTextMessaging

The <Policies.Policy.Data.eas-provisioningdoc.AllowTextMessaging> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device allows the use of SMS or text messaging.

The <Policies.Policy.Data.eas-provisioningdoc.AllowTextMessaging> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowTextMessaging> are listed in the following table.

Value	Description
0	SMS or text messaging is not allowed.
1	SMS or text messaging is allowed.

2.2.2.26 Policies.Policy.Data.eas-provisioningdoc.AllowPOPIMAPEmail

The <Policies.Policy.Data.eas-provisioningdoc.AllowPOPIMAPEmail> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device allows access to POP or IMAP e-mail.

The <Policies.Policy.Data.eas-provisioningdoc.AllowPOPIMAPEmail> element cannot have child elements.

Valid values for The <Policies.Policy.Data.eas-provisioningdoc.AllowPOPIMAPEmail> are listed in the following table.

Value	Description
0	POP or IMAP e-mail access is not allowed.
1	POP or IMAP e-mail access is allowed.

2.2.2.27 Policies.Policy.Data.eas-provisioningdoc.AllowBluetooth

The <Policies.Policy.Data.eas-provisioningdoc.AllowBluetooth> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies the use of Bluetooth on the device.

The <Policies.Policy.Data.eas-provisioningdoc.AllowBluetooth> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowBluetooth> are listed in the following table.

Value	Description
0	Disable Bluetooth.
1	Disable Bluetooth, but allow the configuration of hands-free profiles.
2	Enable Bluetooth.

2.2.2.28 Policies.Policy.Data.eas-provisioningdoc.AllowIrDA

The <Policies.Policy.Data.eas-provisioningdoc.AllowIrDA> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device allows the use of IrDA (infrared) connections.

The <Policies.Policy.Data.eas-provisioningdoc.AllowIrDA> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowIrDA> are listed in the following table.

Value	Description
0	Disable IrDA.
1	Enable IrDA.

2.2.2.29 Policies.Policy.Data.eas-provisioningdoc.RequireManualSyncWhenRoaming

The <Policies.Policy.Data.eas-provisioningdoc.RequireManualSyncWhenRoaming> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device requires manual synchronization when the device is roaming.

The <Policies.Policy.Data.eas-provisioningdoc.RequireManualSyncWhenRoaming> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.RequireManualSyncWhenRoaming> are of those listed in the following table.

Value	Description
0	Do not require manual sync when roaming.
1	Require manual sync when roaming.

2.2.2.30 Policies.Policy.Data.eas-provisioningdoc.AllowDesktopSync

The <Policies.Policy.Data.eas-provisioningdoc.AllowDesktopSync> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device allows synchronization with Desktop ActiveSync.

The <Policies.Policy.Data.eas-provisioningdoc.AllowDesktopSync> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowDesktopSync> are listed in the following table.

Value	Description
0	Do not allow Desktop ActiveSync.
1	Allow Desktop ActiveSync.

2.2.2.31 Policies.Policy.Data.eas-provisioningdoc.MaxCalendarAgeFilter

The <Policies.Policy.Data.eas-provisioningdoc.MaxCalendarAgeFilter> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies the maximum number of calendar days that can be synchronized.

The <Policies.Policy.Data.eas-provisioningdoc.MaxCalendarAgeFilter> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.MaxCalendarAgeFilter> are listed in the following table.

Value	Description
0	All days
4	2 weeks
5	1 month
6	3 months
7	6 months

2.2.2.32 Policies.Policy.Data.eas-provisioningdoc.AllowHTMLEmail

The <Policies.Policy.Data.eas-provisioningdoc.AllowHTMLEmail> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device uses HTML-formatted e-mail.

The <Policies.Policy.Data.eas-provisioningdoc.AllowHTMLEmail> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowHTMLEmail> are listed in the following table.

Value	Description
0	Do not use HTML-formatted e-mail.
1	Use HTML-formatted e-mail.

2.2.2.33 Policies.Policy.Data.eas-provisioningdoc.MaxEmailAgeFilter

The <Policies.Policy.Data.eas-provisioningdoc.MaxEmailAgeFilter> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies the e-mail age limit for synchronization.

The <Policies.Policy.Data.eas-provisioningdoc.MaxEmailAgeFilter> element cannot have child elements.

Valid values are listed in the following table and represent the maximum allowable number of days to sync e-mail.

Value	Description
0	Sync all
1	1 day
2	3 days

Value	Description
3	1 week
4	2 weeks
5	1 month

2.2.2.34 Policies.Policy.Data.eas-provisioningdoc.MaxEmailBodyTruncationSize

The <Policies.Policy.Data.eas-provisioningdoc.MaxEmailBodyTruncationSize> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies the truncation size for plain text–formatted e-mail.

The <Policies.Policy.Data.eas-provisioningdoc.MaxEmailBodyTruncationSize> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.MaxEmailBodyTruncationSize> element MUST be an **integer** of one of the values or ranges listed in the following table.

Value	Description
-1	No truncation.
0	Truncate only the header.
>0	Truncate the e-mail body to the specified size.

2.2.2.35 Policies.Policy.Data.eas-provisioningdoc.MaxEmailHTMLBodyTruncationSize

The <Policies.Policy.Data.eas-provisioningdoc.MaxEmailHTMLBodyTruncationSize> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies the truncation size for HTML-formatted e-mail.

The <Policies.Policy.Data.eas-provisioningdoc.MaxEmailHTMLBodyTruncationSize> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.MaxEmailHTMLBodyTruncationSize> element is an **integer** of one of the values or ranges listed in the following table.

Value	Description
-1	No truncation.
0	Truncate only the header.
>0	Truncate the e-mail body to the specified size.

2.2.2.36 Policies.Policy.Data.eas-provisioningdoc.RequireSignedSMIMEMessages

The <Policies.Policy.Data.eas-provisioningdoc.RequireSignedSMIMEMessages> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device sends signed S/MIME messages.

The <Policies.Policy.Data.eas-provisioningdoc.RequireSignedSMIMEMessages> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.RequireSignedSMIMEMessages> are listed in the following table.

Value	Description
0	Do not send signed S/MIME messages.
1	Send signed S/MIME messages.

2.2.2.37 Policies.Policy.Data.eas-provisioningdoc.RequireEncryptedSMIMEMessages

The <Policies.Policy.Data.eas-provisioningdoc.RequireEncryptedSMIMEMessages> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device sends encrypted e-mail messages.

The <Policies.Policy.Data.eas-provisioningdoc.RequireEncryptedSMIMEMessages> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.RequireEncryptedSMIMEMessages> are listed in the following table.

Value	Description
0	Do not encrypt e-mail messages.
1	Encrypt e-mail messages.

2.2.2.38 Policies.Policy.Data.eas-provisioningdoc.RequireSignedSMIMEAlgorithm

The <Policies.Policy.Data.eas-provisioningdoc.RequireSignedSMIMEAlgorithm> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies the algorithm used when signing S/MIME messages.

The <Policies.Policy.Data.eas-provisioningdoc.RequireSignedSMIMEAlgorithm> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.RequireSignedSMIMEAlgorithm> are listed in the following table.

Value	Description
0	Use SHA.
1	Use MD5.

2.2.2.39 Policies.Policy.Data.eas-provisioningdoc.RequireEncryptionSMIMEAlgorithm

The <Policies.Policy.Data.eas-provisioningdoc.RequireEncryptionSMIMEAlgorithm> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies the algorithm used when encrypting S/MIME messages.

The <Policies.Policy.Data.eas-provisioningdoc.RequireEncryptionSMIMEAlgorithm> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.RequireEncryptionSMIMEAlgorithm> are listed in the following table.

Value	Description
0	3DES algorithm
1	DES algorithm
2	RC2128bit
3	RC264bit
4	RC240bit

2.2.2.40 Policies.Policy.Data.eas-provisioningdoc.AllowSMIMEEncryptionAlgorithmNegotiation

The <Policies.Policy.Data.eas-provisioningdoc.AllowSMIMEEncryptionAlgorithmNegotation> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that controls negotiation of the encryption algorithm.

The <Policies.Policy.Data.eas-provisioningdoc.AllowSMIMEEncryptionAlgorithmNegotation> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowSMIMEEncryptionAlgorithmNegotation> are listed in the following table.

Value	Description
0	Do not negotiate.
1	Negotiate a strong algorithm.
2	Negotiate any algorithm.

2.2.2.41 Policies.Policy.Data.eas-provisioningdoc.AllowSMIMESoftCerts

The <Policies.Policy.Data.eas-provisioningdoc.AllowSMIMESoftCerts> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device can use soft certificates to sign outgoing messages.

The <Policies.Policy.Data.eas-provisioningdoc.AllowSMIMESoftCerts> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowSMIMESoftCerts> are listed in the following table.

Value	Description
0	Do not use soft certificates.
1	Use soft certificates.

2.2.2.42 Policies.Policy.Data.eas-provisioningdoc.AllowBrowser

The <Policies.Policy.Data.eas-provisioningdoc.AllowBrowser> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device allows the use of a web browser.

The <Policies.Policy.Data.eas-provisioningdoc.AllowBrowser> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowBrowser> are listed in the following table.

Value	Description
0	Do not allow the use of a web browser.
1	Allow the use of a web browser.

2.2.2.43 Policies.Policy.Data.eas-provisioningdoc.AllowConsumerEmail

The <Policies.Policy.Data.eas-provisioningdoc.AllowConsumerEmail> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device allows the use of Windows Live.

The <Policies.Policy.Data.eas-provisioningdoc.AllowConsumerEmail> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowConsumerEmail> are listed in the following table.

Value	Description
0	Do not allow the use of Windows Live.
1	Allow the use of Windows Live.

2.2.2.44 Policies.Policy.Data.eas-provisioningdoc.AllowRemoteDesktop

The <Policies.Policy.Data.eas-provisioningdoc.AllowRemoteDesktop> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device allows the use of Remote Desktop.

The <Policies.Policy.Data.eas-provisioningdoc.AllowRemoteDesktop> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowRemoteDesktop> are listed in the following table.

Value	Description
0	Do not allow the use of Remote Desktop.
1	Allow the use of Remote Desktop.

2.2.2.45 Policies.Policy.Data.eas-provisioningdoc.AllowInternetSharing

The <Policies.Policy.Data.eas-provisioningdoc.AllowInternetSharing> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device allows the use of Internet Sharing.

The <Policies.Policy.Data.eas-provisioningdoc.AllowInternetSharing> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowInternetSharing> are listed in the following table.

Value	Description
0	Do not allow the use of Internet Sharing.
1	Allow the use of Internet Sharing.

2.2.2.46 Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList.ApplicationName

The <Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList.ApplicationName> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList** type that specifies the name of an in-ROM application (.exe file) that is not approved for execution.

The **Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList** type has at least one instance of the <Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList.ApplicationName> element.

There is no limit on the number of <Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList.ApplicationName> elements that are defined for a **Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList** type.

2.2.2.47 Policies.Policy.Data.eas-provisioningdoc.ApprovedApplicationList.Hash

The <Policies.Policy.Data.eas-provisioningdoc.ApprovedInApplicationList.Hash> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc.ApprovedInApplicationList** type that specifies the SHA1 hash of an approved in-RAM application.

The **Policies.Policy.Data.eas-provisioningdoc.ApprovedInApplicationList** type has at least one instance of the <Policies.Policy.Data.eas-provisioningdoc.ApprovedInApplicationList.Hash> element.

There is no limit on the number of <Policies.Policy.Data.eas-provisioningdoc.ApprovedInApplicationList.Hash> elements that are defined for a **Policies.Policy.Data.eas-provisioningdoc.ApprovedInApplicationList** type.

3 Protocol Details

3.1 Client Details

3.1.1 Abstract Data Model

This section describes a conceptual model of possible data organization that an implementation maintains to participate in this protocol. The described organization is provided to facilitate the explanation of how the protocol behaves. This document does not mandate that implementations adhere to this model as long as their external behavior is consistent with that described in this document.

The **Provision** command enables client devices to request from the server the security policy settings that the server administrator sets.

The client ensures that the security policy settings are actually enforced. The server SHOULD enforce that the client device has requested the policy settings before the client is allowed to synchronize with the server. The server relies on the client to apply the policy settings on the client device.

There are two phases to the **Provision** command: request and download of policy settings, and acknowledgement that the policy settings have been received and applied. Before synchronizing with the server, the client device requests the policy settings from the server. After it receives the policy settings or **remote wipe** directive from the server in the **Provision** command response, the client device issues an acknowledgement that indicates success or failure in receipt and intent to comply with the settings. The acknowledgement phase of the **Provision** command request varies depending on the context.

Clients SHOULD NOT use the **Provision** command without having unsuccessfully tried to communicate with the server. For example, a device might request provisioning after it receives a 449 response to a **Sync** request.

The current policy information on the client is a unique unsigned **integer**, which is sent to the server in the X-MS-PolicyKey of the HTTP header of all protocol commands except for the **Ping** and **Options** commands. If the policy key of the client is out of date, the server returns an HTTP 449 status code. The client then issues a new **Provision** command to obtain the latest policy key.

Note that the only <PolicyKey> element value that the client can successfully use is the key that it obtained from the most recent server response to the acknowledgement phase of the provisioning session. The PolicyKey from the initial **Provision** command is temporary and can only be used to obtain a more permanent key. This temporary policy key cannot be used to verify that the client has complied with the policy that is set on the server.

3.1.2 Timers

None.

3.1.3 Initialization

None.

3.1.4 Higher-Layer Triggered Events

None.

3.1.5 Message Processing Events and Sequencing Rules

3.1.5.1 Provision Command

The **Provision** command is specified in [MS-ASCMD] section 2.2.1.12.

3.1.5.2 Provision Command Errors

Code	Meaning	Cause	Scope	Resolution
1	Success.	The requested policy data is included in the response.	Policy	Apply the policy.
2	Protocol error.	Syntax error in the Provision command request.	Global	Fix bug in client code.
2	Policy not defined.	No policy of the requested type is defined on the server.	Policy	Stop sending policy information. No policy is implemented.
3	The policy type is unknown.	The client sent a policy that the server does not recognize.	Policy	Issue a request by using MS-EAS-Provisioning-WBXML
3	An error occurred on the server.	Server misconfiguration, temporary system issue, or bad item. This is frequently a transient **condition**.	Global	Retry.
4	The policy data is corrupted.	The policy data on the server is corrupted.	Policy	Direct the user to contact the server administrator.
5	Policy key mismatch.	The client is trying to acknowledge an out-of-date or invalid policy.	Policy	Issue a new **Provision** request to obtain a valid policy key.

3.1.6 Timer Events

None.

3.1.7 Other Local Events

None.

3.2 Server Details

3.2.1 Abstract Data Model

This section describes a conceptual model of possible data organization that an implementation maintains to participate in this protocol. The described organization is provided to facilitate the explanation of how the protocol behaves. This document does not mandate that implementations adhere to this model as long as their external behavior is consistent with that described in this document.

The server enforces that the client device has requested the policy settings before the client is allowed to synchronize with the server. The server relies on the client to apply the policy settings on the client device.

The **Provision** command also supports remote wipe. At the request of a server administrator, a given device can have its memory wiped. On the next request, the device will receive a prompt to refresh its policy settings. The policy settings will include a request from the server to wipe the local memory of the client device.

The server tracks a shared policy key, which identifies the policy for the client. The policy key is provided to the server after the policy has been generated. If there is a mismatch between the server and client policy keys, the server detects that the policy has been changed, or if the administrator has directed that the device be wiped, the server returns a custom HTTP 449 (Need Provisioning) response. When the client receives the custom HTTP 449 response, the client will execute the Provision command to update the policy, thereby obtaining the policy settings, a remote wipe directive, or both.

3.2.2 Timers

None.

3.2.3 Initialization

None.

3.2.4 Higher-Layer Triggered Events

None.

3.2.5 Message Processing Events and Sequencing Rules

3.2.5.1 Provision Command

The **Provision** command is specified in [MS-ASCMD] section 2.2.1.12.

3.2.5.2 Provision Command Errors

Code	Meaning	Cause	Scope	Resolution
1	Success.	The requested policy data is included in the response.	Policy	Apply the policy.
2	Protocol error.	Syntax error in the Provision command request.	Global	Fix bug in client code.
2	Policy not defined.	No policy of the requested type is defined on the server.	Policy	Stop sending policy information. No policy is implemented.
3	The policy type is unknown.	The client sent a policy that the server does not recognize.	Policy	Issue a request by using MS-EAS-Provisioning-WBXML.
3	An error occurred on the server.	Server misconfiguration, temporary system issue, or bad item. This is frequently a transient condition.	Global	Retry.
4	The policy data is corrupted.	The policy data on the server is corrupted.	Policy	Direct the user to contact the server administrator.

Code	Meaning	Cause	Scope	Resolution
5	Policy key mismatch.	The client is trying to acknowledge an out-of-date or invalid policy.	Policy	Issue a new **Provision** request to obtain a valid policy key.

3.2.6 Timer Events

None.

3.2.7 Other Local Events

None.

4 Protocol Examples

Please note that the sample request/responses do not show the base64-encoding of the **URI** query parameters and WBXML-encoding of the XML bodies for the sake of clarity.

4.1 Downloading the Current Server Security Policy

This section provides a walkthrough of the messages that are used to download the current server security policy. This section contains the following:

- Phase 1: Enforcement
- Phase 2: Client Downloads **Policy** from Server
- Phase 3: Client Acknowledges Receipt and Application of Policy Settings
- Phase 4: Client Performs **FolderSync** by Using the Final <PolicyKey>

4.1.1 Phase 1: Enforcement

In the following example, the client tries the **FolderSync** command, which is denied by the server <1> because the server has determined that the device does not have the current policy (as denoted by the X-MS-PolicyKey header). The server returns HTTP 200 (ok) with a global status code in the body of the response of 142.

Request

```
POST Microsoft-Server- ActiveSync?User=deviceuser&DeviceId=6F24CAD599A5BF1A690246B8C68FAE8D
&DeviceType=PocketPC&Cmd=FolderSync
Accept-Language: en-us
MS-ASProtocolVersion: 14.0
Content-Type: application/vnd.ms-sync.wbxml
X-MS-PolicyKey: 0

<?xml version="1.0" encoding="utf-8"?>
<FolderSync xmlns="FolderHierarchy:">
<SyncKey>0</SyncKey>
</FolderSync>
```

4.1.2 Phase 2: Client Downloads Policy from Server

In this phase, the client downloads the policy from the server and receives a temporary <PolicyKey>. The client will later use the <PolicyKey> to acknowledge the policy and in doing so obtain a key that will enable the client to successfully execute protocol commands against the server.

Request

```
POST Microsoft-Server-
ActiveSync?User=deviceuser&DeviceId=6F24CAD599A5BF1A690246B8C68FAE8D&DeviceType=PocketPC&Cmd=
Provision
Accept-Language: en-us
MS-ASProtocolVersion: 14.0
Content-Type: application/vnd.ms-sync.wbxml
X-MS-PolicyKey: 0
```

```
<?xml version="1.0" encoding="utf-8"?>
<Provision xmlns="Provision:">
     <Policies>
          <Policy>
               <PolicyType> MS-EAS-Provisioning-WBXML</PolicyType>
          </Policy>
     </Policies>
</Provision>
```

Response

```
HTTP/1.1 200 OK
Connection: Keep-Alive
Content-Length: 1069
Date: Mon, 01 May 2006 20:15:15 GMT
Content-Type: application/vnd.ms-sync.wbxml
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
MS-Server-ActiveSync: 8.0
Cache-Control: private

<?xml version="1.0" encoding="utf-8"?>
<Provision xmlns="Provision:">
     <Status>1</Status>
     <Policies>
          <Policy>
               <PolicyType>MS-EAS-Provisioning-WBXML</PolicyType>
               <Status>1</Status>
               <PolicyKey>1307199584</PolicyKey>
               <Data>
                    <eas-provisioningdoc>
                         <DevicePasswordEnabled>1
                         </DevicePasswordEnabled>
                         <AlphanumericDevicePasswordRequired>1
</AlphanumericDevicePasswordRequired> <PasswordRecoveryEnabled>1
                         </PasswordRecoveryEnabled> <DeviceEncryptionEnabled>1
                         </DeviceEncryptionEnabled> <AttachmentsEnabled>1
                         </AttachmentsEnabled> <MinDevicePasswordLength/>
<MaxInactivityTimeDeviceLock>333 </MaxInactivityTimeDeviceLock>
<MaxDevicePasswordFailedAttempts>8 </MaxDevicePasswordFailedAttempts> <MaxAttachmentSize/>
<AllowSimpleDevicePassword>0
                         </AllowSimpleDevicePassword> <DevicePasswordExpiration/>
<DevicePasswordHistory>0
                         </DevicePasswordHistory>
                    </eas-provisioningdoc>
               </Data>
          </Policy>
     </Policies>
</Provision>
```

4.1.3 Phase 3: Client Acknowledges Receipt and Application of Policy Settings

The client acknowledges the policy download and policy application by using the temporary <PolicyKey> obtained in phase 2. In this case, the client has indicated compliance and provided the

correct <PolicyKey>. Therefore, the server responds with the "final" <PolicyKey> which the client then uses in the X-MS-PolicyKey header of successive command requests to satisfy policy enforcement.

Request

```
POST Microsoft-Server-
ActiveSync?User=deviceuser&DeviceId=6F24CAD599A5BF1A690246B8C68FAE8D&DeviceType=PocketPC&Cmd=
Provision
Accept-Language: en-us
MS-ASProtocolVersion: 14.0
Content-Type: application/vnd.ms-sync.wbxml
X-MS-PolicyKey: 1307199584

<?xml version="1.0" encoding="utf-8"?>
<Provision xmlns="Provision:">
     <Policies>
          <Policy>
               <PolicyType> MS-EAS-Provisioning-WBXML</PolicyType>
<PolicyKey>1307199584</PolicyKey>
               <Status>1</Status>
          </Policy>
     </Policies>
</Provision>
```

Response

```
HTTP/1.1 200 OK
Connection: Keep-Alive
Content-Length: 63
Date: Mon, 01 May 2006 20:15:17 GMT
Content-Type: application/vnd.ms-sync.wbxml
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
MS-Server-ActiveSync: 8.0
Cache-Control: private

<?xml version="1.0" encoding="utf-8"?>
<Provision xmlns="Provision:">
     <Status>1</Status>
          <Policies>
               <Policy>
                    <PolicyType> MS-EAS-Provisioning-WBXML </PolicyType>
               <Status>1</Status>
               <PolicyKey>3942919513</PolicyKey>
          </Policy>
     </Policies>
</Provision>
```

4.1.4 Phase 4: Client Performs FolderSync by Using the Final PolicyKey

The client uses the "final" policy key obtained in phase 3 in the header of the **FolderSync** command request.

Request

```
POST Microsoft-Server-
ActiveSync?User=deviceuser&DeviceId=6F24CAD599A5BF1A690246B8C68FAE8D&DeviceType=PocketPC&Cmd=
Provision
Accept-Language: en-us
MS-ASProtocolVersion: 14.0
Content-Type: application/vnd.ms-sync.wbxml
X-MS-PolicyKey: 3942919513

<?xml version="1.0" encoding="utf-8"?>
<FolderSync xmlns="FolderHierarchy:">
     <SyncKey>0</SyncKey>
</FolderSync>
```

4.2 Directing a Client to Execute a Remote Wipe

The following example shows a set of remote wipe **Requests** and their corresponding **Responses**.

4.2.1 Step 1 Request

```
POST /Microsoft-Server-
ActiveSync?Cmd=FolderSync&User=T0SyncUser1v14.0&DeviceId=Device1&DeviceType=PocketPC HTTP/1.1
Content-Type: application/vnd.ms-sync.wbxml
MS-ASProtocolVersion: 14.0
X-MS-PolicyKey: 0
User-Agent: ASOM
Host: EXCH-B-003

<?xml version="1.0" encoding="utf-8"?>
<FolderSync xmlns="FolderHierarchy:">
     <SyncKey>0</SyncKey>
</FolderSync>
```

4.2.2 Step 1 Response

```
HTTP/1.1 200 OK
Content-Type: application/vnd.ms-sync.wbxml
X-MS-MV: 14.0.511
Date: Wed, 25 Mar 2009 01:23:58 GMT
Content-Length: 15

<?xml version="1.0" encoding="utf-8"?>
<FolderSync >
     <Status>140</Status>
</FolderSync>
```

4.2.3 Step 2 Request

```
POST /Microsoft-Server-
ActiveSync?Cmd=Provision&User=T0SyncUser1v14.0&DeviceId=Device1&DeviceType=PocketPC HTTP/1.1
Content-Type: application/vnd.ms-sync.wbxml
MS-ASProtocolVersion: 14.0
X-MS-PolicyKey: 0
User-Agent: ASOM
```

```
Host: EXCH-B-003

<?xml version="1.0" encoding="utf-8"?>
<Provision></Provision>
```

4.2.4 Step 2 Response

```
HTTP/1.1 200 OK
Content-Type: application/vnd.ms-sync.wbxml
X-MS-MV: 14.0.511
Date: Wed, 25 Mar 2009 01:23:58 GMT
Content-Length: 14

<?xml version="1.0" encoding="utf-8"?>
<Provision>
<Status>1</Status>
<RemoteWipe />
</Provision>
```

4.2.5 Step 3 Request

```
POST /Microsoft-Server-
ActiveSync?Cmd=Provision&User=T0SyncUser1v14.0&DeviceId=Device1&DeviceType=PocketPC HTTP/1.1
Content-Type: application/vnd.ms-sync.wbxml
MS-ASProtocolVersion: 14.0
X-MS-PolicyKey: 0
User-Agent: ASOM
Host: EXCH-B-003

<?xml version="1.0" encoding="utf-8"?>
<Provision>
    <RemoteWipe>
        <Status>1</Status>
    </RemoteWipe>
</Provision>
```

4.2.6 Step 3 Response

```
HTTP/1.1 200 OK
Content-Type: application/vnd.ms-sync.wbxml
X-MS-MV: 14.0.511
Date: Wed, 25 Mar 2009 01:24:01 GMT
Content-Length: 14

<?xml version="1.0" encoding="utf-8"?>
<Provision>
<Status>1</Status>
<RemoteWipe />
</Provision>
```

5 Security

5.1 Security Considerations for Implementers

None.

5.2 Index of Security Parameters

None.

6 Appendix A: Product Behavior

The information in this specification is applicable to the following product versions. References to product versions include released service packs.

- Microsoft Exchange Server 2007
- Microsoft Exchange Server 2010

Exceptions, if any, are noted below. If a service pack number appears with the product version, behavior changed in that service pack. The new behavior also applies to subsequent service packs of the product unless otherwise specified.

Unless otherwise specified, any statement of optional behavior in this specification prescribed using the terms SHOULD or SHOULD NOT implies product behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term MAY implies that product does not follow the prescription.

<1> Section 4.1.1: Exchange 2007 returns status code HTTP 449.

7 Change Tracking

No table of changes is available. The document is either new or has had no changes since its last release.

8 Index